**UNIVERSIDADE ESTADUAL PAULISTA**
**"JÚLIO DE MESQUITA FILHO"**
**Faculdade de Ciências Humanas e Sociais**
**Campus de Franca - SP**

Vanessa Paula dos Santos

# A LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018, E O ATENDIMENTO AO PRINCÍPIO DA NÃO DISCRIMINAÇÃO

FRANCA – S.P.
2023

VANESSA PAULA DOS SANTOS

# A LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018, E O ATENDIMENTO AO PRINCÍPIO DA NÃO DISCRIMINAÇÃO

Dissertação apresentada ao Programa de Pós-graduação em Planejamento e Análise de Políticas Públicas, da Faculdade de Ciências Humanas e Sociais – Unesp/Franca, como requisito para obtenção do título de mestre.

**Linha de pesquisa:** Instituições, Cidadania e Políticas Sociais.
**Orientador:** Prof. Dr. Agnaldo de Sousa Barbosa.

FRANCA – S.P.
2023

S237l

Santos, Vanessa Paula dos
A LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018, E O ATENDIMENTO AO PRINCÍPIO DA NÃO DISCRIMINAÇÃO / Vanessa Paula dos Santos. -- Franca, 2023
153 p.

Dissertação (mestrado profissional) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências Humanas e Sociais, Franca
Orientadora: Agnaldo de Sousa Barbosa

1. Lei Geral de Proteção de Dados Pessoais LGPD. 2. Princípio da Não Discriminação. 3. Política Pública Regulatória. 4. Política e Direito. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências Humanas e Sociais, Franca. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

VANESSA PAULA DOS SANTOS

**A Lei Geral de Proteção de Dados - Lei nº 13.709/2018, e o atendimento ao princípio da não discriminação**

Dissertação apresentada ao Programa de Pós-graduação em Planejamento e Análise de Políticas Públicas, da Faculdade de Ciências Humanas e Sociais – Unesp/Franca, como requisito para obtenção do título de mestre.
Linha de pesquisa: Instituições, Cidadania e Políticas Sociais.

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Agnaldo de Sousa Barbosa
Universidade Estadual Paulista "Júlio de Mesquita Filho"- UNESP

_____

Banca: Profª. Drª. Luciana Lopes Canavez
Universidade Estadual Paulista "Júlio de Mesquita Filho"- UNESP

_____

Banca: Profª. Drª Bianca Kremer
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP

Franca – SP. 27 de setembro de 2023.

## IMPACTO POTENCIAL DESTA PESQUISA

Tendo como base o entendimento sobre o princípio antidiscriminatório e dos motivos que levaram a sua inserção na Lei Geral de Proteção de Dados Pessoais, pretende-se identificar com base nesta pesquisa qual a relação entre as ações judiciais que utilizam como fundamento este princípio nas decisões proferidas por magistrados bem como observar quais as medidas que estão sendo tomadas para que este seja atendido. Desta forma, a presente pesquisa pretende contribuir para a criação de possíveis alternativas para a diminuição das discriminações ilícitas e abusivas até então presentes no tratamento de dados pessoais.

## POTENTIAL IMPACT OF THIS RESEARCH

Based on the understanding of the anti-discrimination principle and the reasons that led to its inclusion in the General Law for the Protection of Personal Data, it is intended to identify, based on this research, the relationship between the lawsuits that use this principle as a basis in the decisions handed down by magistrates as well as observe what measures are being taken to ensure that this is met. In this way, the present research intends to contribute to the creation of possible alternatives for the reduction of illicit and abusive discrimination hitherto present in the processing of personal data.

**DEDICATÓRIA**

*À Luisa e à Alicia, minhas filhas. Que vocês possam moldar a própria vida e caminhar com os próprios passos.*

**AGRADECIMENTOS**

Gostaria de expressar minha mais profunda gratidão a todos que contribuíram para a realização deste trabalho de pesquisa e para a conclusão deste mestrado.

Primeiramente, à minha família, que sempre acreditou em mim e me apoiou em todas as etapas da minha jornada acadêmica, quero expressar meu amor e minha eterna gratidão. Pai e mãe, suas palavras de incentivo foram fundamentais para minha motivação. Caio, estar ao seu lado no meio da tempestade ou do sol, sempre me estimulou a nunca desistir. Vanúcia, minha irmã, que cuidou das minhas filhas como se fossem suas para que eu pudesse pesquisar nos finais de semana que precisei. Fica aqui transformado em palavras o meu amor eterno por vocês.

Ao meu orientador, por sua orientação, apoio incansável e valiosos insights ao longo desta pesquisa. Sua dedicação à excelência acadêmica foi e é uma fonte constante de inspiração.

Ao grupo de pesquisa Pensar Negro, que surgiu de um projeto pensado por mim e pelo meu orientador, obrigada por compartilharem suas ideias, discussões estimulantes e momentos de aprofundamento e descontração que tornaram essa jornada mais enriquecedora.

Às instituições de pesquisa, bibliotecas e órgãos de financiamento que forneceram recursos e acesso a materiais essenciais para esta pesquisa, meu sincero agradecimento.

Aos meus ancestrais, que mesmo em memória, me impulsionam com as suas histórias de luta, especialmente as minhas avós e bisavós que lutaram para que suas famílias se mantivessem fortes mesmo diante das adversidades.

Por último, mas não menos importante, quero agradecer aos amigos e a todos os que de alguma forma me apoiaram ao longo deste percurso acadêmico, mesmo nos momentos mais desafiadores.

Esta pesquisa não teria sido possível sem a ajuda e o apoio de todas essas pessoas e instituições. Expresso minha profunda gratidão a todos vocês**.**

**RESUMO**

Os princípios presentes nas legislações brasileiras são tidos como base da interpretação das normas. E um dos princípios que a Lei Geral de Proteção de Dados (LGPD) traz em seu ordenamento é o princípio da não discriminação (artigo 6º, IX). A LGPD iniciou sua vigência em todo o território brasileiro no dia 18 de setembro de 2020, e se baseou em uma norma da União Europeia, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), que também possui como um dos seus princípios o da não discriminação. Com a inserção do referido princípio em leis de tratamento de dados busca-se a diminuição das desigualdades que podem ser geradas em ambientes que exigem o colhimento de dados, já que a não discriminação significa a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. E se analisarmos as decisões que são tomadas com base nos dados por meios automatizados, que chegam a conclusões sem qualquer envolvimento humano, é possível inferir que, certamente, uns são mais prejudicados que outros devido ao tratamento incorreto do dado que não obedeceu ao princípio da não discriminação. São exemplos, o colhimento de dados biométricos, a decisão de conceder um financiamento ou empréstimo a um indivíduo, o resultado de um teste de aptidão de recrutamento que usa algoritmos e critérios pré-programados ou até mesmo o sistema de saúde que se utiliza de dados fornecidos por seus titulares em farmácias, para determinar, por exemplo, o valor do plano privado de saúde. Assim, com este trabalho prioriza a análise crítica do artigo 6º, IX, da LGPD e também dos principais conceitos e leis que ordenam o atendimento ao princípio da não discriminação, bem como, verifica no Tribunal de Justiça de São Paulo quais decisões judiciais tiveram por base em suas fundamentações esta tutela antidiscriminatória. A partir daí pretende-se acompanhar a mobilização desta política regulatória – LGPD – com o objetivo de destacar caminhos e alternativas para a mitigação das discriminações abusivas e ilícitas que ocorrem no colhimento e tratamento de dados pessoais.

**Palavras-chave:** Dados Pessoais; Política Pública Regulatória; Princípio da Não Discriminação; Análise Decisões Judiciais; Lei Geral de Proteção de Dados Pessoais; LGPD.

**ABSTRACT**

The principles present in Brazilian legislation are taken as the basis for interpreting standards. And one of the principles that the General Data Protection Law (LGPD) brings into its structure is the principle of non-discrimination (article 6, IX). The LGPD came into effect throughout the Brazilian territory on September 18, 2020, and was based on a European Union standard, the General Data Protection Regulation (GDPR, 2016), which also has as one of its principles that of non-discrimination. With the inclusion of the aforementioned principle in data processing laws, we seek to reduce inequalities that can be generated in environments that require data collection, since non-discrimination means the impossibility of carrying out processing for illicit or abusive discriminatory purposes. . And if we analyze the decisions that are made based on data by automated means, which reach conclusions without any human involvement, it is possible to infer that, certainly, some are more harmed than others due to the incorrect treatment of data that did not comply with the principle of non-discrimination. Examples include the collection of biometric data, the decision to grant financing or a loan to an individual, the result of a recruitment aptitude test that uses pre-programmed algorithms and criteria or even the healthcare system that uses data provided by their holders in pharmacies, to determine, for example, the value of the private health plan. Thus, this work prioritizes the critical analysis of article 6, IX, of the LGPD and also of the main concepts and laws that order compliance with the principle of non-discrimination, as well as verifying in the Court of Justice of São Paulo which judicial decisions were This anti-discrimination protection is based on its foundations. From then on, the aim is to monitor the mobilization of this regulatory policy – LGPD – with the aim of highlighting paths and alternatives for mitigating abusive and illicit discrimination that occurs in the collection and processing of personal data.

**Keywords:** Personal data; Regulatory Public Policy; Principle of Non-Discrimination; Analysis of Judicial Decisions; General Personal Data Protection Law; LGPD.

**SUMÁRIO**

**INTRODUÇÃO**.....12

1. **PERSPECTIVAS PARA ENFRENTAMENTO DE UM DESAFIO COLETIVO NA CONTEMPORANEIDADE: O PRINCÍPIO DA NÃO DISCRIMINAÇÃO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.....17**

**1.1 Contextualização sociocultural e necessidade de inserção da não discriminação na LGPD** .....17

**1.2 Panorama do princípio da não discriminação nas leis nacionais e Internacionais.**.....21

**2.DISCRIMINAÇÕES BASEADAS NO USO DE DADOS PESSOAIS**.....29

**2.1 Reconhecimento facial**.....31
**2.2 *Score* de crédito** .....37
**2.3 Processos seletivos de acesso a vagas de empregos**.....39

**3. A ATUAÇÃO DO PODER JUDICIÁRIO PARA ATENDIMENTO AO PRINCÍPIO DA NÃO DISCRIMINAÇÃO**.....41

**3.1 As decisões judiciais de Primeiro Grau do Tribunais do Estado de São Paulo** .....42
**3.1.1 Ajuizamento de Ação Civil Pública contra o Uso de Reconhecimento Facial pela Companhia do Metropolitano de São Paulo - Processo nº 1090663-42.2018.8.26.0100 – 37ª VARA CÍVEL – Foro Central. Ação Civil Pública**.....44
**3.1.2 Apelação nº 1001822-16.2021.8.26.0246 da 2ª Vara do Foro de Ilha Solteira. Procedimento Comum Cível. Práticas Abusivas. Voto 2.384**.....48

**4. MOBILIZAÇÃO POLÍTICA E DIREITO: IMPLEMENTAÇÃO DE UMA POLÍTICA PÚBLICA REGULATÓRIA COMO FORMA DE ADAPTAÇÃO A NOVA REALIDADE DE COLHIMENTO DOS DADOS PESSOAIS** .....54
**4.1 Conceito de política pública regulatória** .....54
**4.2 As limitações e as potencialidades da aplicabilidade deste conceito à realidade brasileira**.....56

**CONCLUSÃO** .....59

**REFERÊNCIAS BIBLIOGRÁFICAS E ELETRÔNICAS.....**.....61

**ANEXOS**.....66
1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.....66
2 - ACÓRDÃO DA 8ª CÂMARA DE DIREITO PÚBLICO – TJSP - AGRAVO DE INSTRUMENTO NO PROCESSO Nº 1090663-42.2018.8.26.0100.....103
3 – ACÓRDÃO DA 38ª CÂMARA DE DIREITO PRIVADO – TJSP – APELAÇÃO NO PROCESSO Nº 1001822-16.2021.8.26.0246.....151

## INTRODUÇÃO

A área de proteção e privacidade de dados pessoais ganhou espaço recentemente no Brasil em decorrência de uma forte tendência mundial em proteger uma realidade inescapável que utiliza dados para obtenção de vantagens econômicas e até mesmo políticas, bem como também é vista como o principal ativo para a formulação de políticas públicas.

Com a ascensão das novas tecnologias da informação e comunicação, nos diz Santos que:

> O volume de troca de informações tornou-se expressivo na sociedade e, nesse sentido, fizeram-se necessárias políticas públicas regulatórias para se tratar o assunto, observando-se, dentre outros, aspectos relacionados à privacidade, à transparência e à forma como os dados são tratados por instituições (públicas e privadas), com vistas a proteger os direitos fundamentais da privacidade e da liberdade (SANTOS, 2020).

Desta forma, a proteção dos dados pessoais se relaciona diretamente com a privacidade, pois, como nos diz Carissa Véliz, a "privacidade é importante porque a falta dela dá aos outros poder sobre você", e assim prossegue:

> Existe uma conexão estreita entre poder e conhecimento. No mínimo, o conhecimento é um instrumento de poder. O filósofo estadista inglês Francis Bacon, entendia que o conhecimento em si é uma forma de poder. Mais de três séculos depois, o historiador francês Michel Focault foi ainda mais longe e argumentou que o poder produz conhecimento tanto quanto o contrário. Há poder no conhecimento e conhecimento no poder. O poder gera conhecimento e decide o que conta como conhecimento. Através da coleta de seus dados e do aprendizado sobre você, o Google se fortalece, e esse poder permite ao Google decidir o que conta como conhecimento sobre você através do uso de seus dados pessoais. Se o Google classifica você como um homem de meia-idade sem um diploma universitário e que sofre de ansiedade, digamos, *isso* conta como conhecimento sobre você através – mesmo que esteja completamente errado, ou fora de contexto, ou desatualizado, ou irrelevante. Através da proteção de nossa privacidade, impedimos que outras pessoas tenham o poder de certos conhecimentos a nosso respeito que possam ser utilizados contra nossos interesses. Tendo mais poder, podemos decidir no que conta como conhecimento. Devemos poder decidir em parte o que conta como conhecimento sobre nós mesmos; devemos ter uma opinião sobre o que os outros estão autorizados a aprender ou inferir sobre nós (VÉLIZ, 2021, p. 78 e 82-83).

É fato que a tecnologia se faz cada vez mais presente no cotidiano das pessoas. Somos rodeados por televisores, computadores, tablets, celulares; passamos o dia conectados com outros indivíduos por meio da internet e das mais diversas redes sociais. Atualmente, além das funcionalidades já citadas, a tecnologia também pode fazer escolhas em nosso lugar – algoritmos já são suficientemente desenvolvidos para tomarem, autonomamente, decisões baseadas em um banco de dados que a eles for fornecido. E esta tecnologia presente no nosso

dia a dia não visa a proteção dos dados pessoais, da privacidade e nem tampouco contribui para que discriminações negativas sejam banidas da atualidade, ou seja, um sistema pode perpetuar as desigualdades existentes no mundo.

Como exemplo do que foi dito acima, podemos apontar o uso de algoritmos para coleta e armazenamento de dados. Mas o que são algoritmos? Segundo o artigo "Controvérsias sobre Danos Algorítmicos: discursos corporativos sobre discriminação codificada", publicado na Revista Observatório:

> Algoritmos nunca agem isoladamente (SEAVER, 2019; SILVEIRA, 2019). Definidos, em geral, como um conjunto de instruções ou regras para solucionar um problema ou para realizar uma tarefa, precisam estar em contato com uma estrutura de dados para agirem. Algoritmos integram uma rede de actantes (LATOUR, 2005). Suas conexões com dados de entrada, com o feedback, com os efeitos de suas próprias decisões e com os demais componentes dos sistemas que os implementam precisam ser considerados.
> (...) Esses sistemas podem ser confeccionados para seguirem regras de como executar suas ações a partir das informações que recebem. Podem ser criados para aprenderem com os dados que recebem em função dos objetivos prescritos. Também podem ter como finalidade encontrar correlações fortes nos dados que recebem. Enfim, podem criar suas operações com base nos dados e não em regras fixadas. (SILVA; SILVEIRA, 2020, p. 1/2)

Neste sentido, a matemática e ativista Cathy O'Neil, afirma que os algoritmos são "opiniões fechadas em matemática" (O'NEIL, 2020) e, segundo ela, dependendo de quem construa esses modelos, quais variáveis leva em conta, e com que dados os alimente, o resultado será um ou outro. Segundo observa: "Geralmente achamos que os algoritmos são neutros, mas não é assim". Ou então, conforme explica Virginia Eubanks "Os vieses são estruturais e sistêmicos, têm pouco a ver com uma decisão individual" (PASCUAL, Manuel G ).

Dessa forma, quando para o tratamento de dados for utilizada a leitura por algoritmo, possivelmente este se baseará em um padrão, que poderá ser discriminatório, se não observada igualdade de oportunidades em razão de raça, sexo e outros dados passíveis de discriminação, que a LGPD nomeia como sensíveis.

Entre os vários exemplos práticos de casos públicos relacionados ao não atendimento ao princípio da não discriminação temos o caso da *Amazon*, que com base no histórico de contratações levou à discriminação de mulheres na seleção pela ferramenta utilizada:

> (...) a *Amazon* foi acusada de ter criado um algoritmo de recrutamento de novos empregados que "aprendeu" que candidatos homens eram preferíveis em detrimento das mulheres. Sobre isso, a gigante norte-americana preferiu não responder às acusações. No mesmo sentido, um estudo publicado na revista *Science* em 2017 revela que sistemas baseados em *machine learning* replicam os mesmos estereótipos de gênero e raça que os humanos lutam para controlar. De onde estes estereótipos vem?

> No caso do algoritmo da *Amazon*, o problema se materializou porque o sistema foi treinado com currículos submetidos à análise da empresa durante os dez anos anteriores, e a maioria deles veio de homens. Ou seja, o algoritmo em si não era enviesado, mas a base de dados que foi utilizada, sim. (SARAIVA, 2019)

Ou então, podemos também utilizar outro exemplo que ocorreu no ano de 2019, onde:

> Em julho daquele mesmo ano, foi a hora da polícia do Rio iniciar seu projeto de reconhecimento facial. Escolheu-se o bairro de Copacabana como área de testes, e diversos postes foram instalados em pontos espalhados pelo bairro, devidamente equipados com câmeras nas suas extremidades. No segundo dia de testes, uma mulher foi reconhecida como sendo Maria Lêda Félix da Silva, condenada por homicídio e procurada pela polícia. Imediatamente os policiais conduziram a mulher que dizia não ser a procurada, mas estava sem documentação, até a delegacia. O erro foi resolvido quando familiares da mulher conseguiram encontrá-la na delegacia e, de posse dos seus documentos, conseguiram provar que ela não era a mulher procurada. O caso é mais um de uma série de erros que essas tecnologias cometem, mas tem um agravante: Maria Lêda, a "procurada", já estava cumprindo pena em presídio havia quatro anos. Não só os algoritmos erraram, mas também a polícia que utilizou um banco de dados desatualizado.
>
> Os projetos foram avançando por estados e municípios sem encontrar muita resistência. No final de 2019 eu já tinha coletado mais de 150 prisões com o uso de reconhecimento facial, e nos casos onde havia informações, mais de 90% das pessoas eram negras, a maioria presas por crimes sem violência. As poucas vozes que se colocaram de maneira crítica à adoção desses algoritmos pelas polícias brasileiras não foram suficientes para que um debate nacional fosse pautado. Mas quais são os problemas?
>
> Algoritmos são como receitas de bolo, instruções a serem seguidas para atingir o resultado final. O que acontece é que muitos desses códigos são criados com base em grandes bancos de dados por meio do aprendizado de máquina. No caso do reconhecimento facial, um grande banco de imagens de rostos é usado para ensinar o algoritmo a identificar o que é um rosto. (NUNES, 2021)

Sendo assim, a utilização dos dados pessoais e da tecnologia deve estar alinhada com os princípios não só da LGPD, mas também com os relacionados à dignidade humana, pois, como bem observa Véliz:

> A narrativa de que a tecnologia é progressiva e inevitável é complacente e enganosa. O poder produz o conhecimento, as narrativas e a racionalidade que o favorecem e o sustentam. A tecnologia nos conta as histórias que a fazem parecer ao mesmo tempo indispensável e boa. Mas parte da tecnologia desenvolvida nas últimas décadas não tem sido minimamente progressista – ela tem contribuído para perpetuar as tendências sexistas e racistas. (2021, p. 93)

A sobrevivência fica ameaçada em uma sociedade que ainda discrimina gêneros, sexualidade e raça. Isso traz a necessidade de que sejam feitas constantemente análises das novas ferramentas tecnológicas e não tecnológicas, para constatar se elas contribuem ou não para a diminuição destas discriminações. E a LGPD poderá contribuir e muito para o decréscimo dos altos índices que colocam o Brasil entre os países que mais discriminam. Assim,

analisar o acesso ou a forma com que os dados pessoais são tratados e manipulados se torna um imperativo para a manutenção de garantias democráticas.

Outrossim, devemos, igualmente, observar a forma com que os dados são tratados e colhidos pela administração pública na execução de políticas públicas, se realmente obedece ao princípio da não discriminação.

A definição de Políticas Públicas apresentada por Guareschi diz que elas são:

> [...] o conjunto de ações coletivas voltadas para a garantia dos direitos sociais, configurando um compromisso público que visa dar conta de determinada demanda, em diversas áreas. Expressa a transformação daquilo que é do âmbito privado em ações coletivas no espaço público (2004, p. 180).

Conforme outros autores que classificam as políticas públicas, e que abordam alguns critérios para abranger a enorme gama de temas e variáveis que as influenciam, é nos mostrado que há diversas tipologias:

> A tipologia de Lowi, autor responsável por uma revolução na relação causal entre o exercício político e a política pública, fundamenta-se no impacto que a política pública pretende ter na sociedade, criando, portanto, quatro tipos: políticas regulatórias, que determinam os padrões de comportamento da sociedade; políticas distributivas, que direcionam recursos difusos da coletividade para grupos específicos de interesses; políticas redistributivas, que concedem benefícios a um grupo específico, retirando recursos de outros grupos também específicos de atores; e as políticas constitutivas, que definem as regras que irão moldar o funcionamento da sociedade e do governo. (MUZZI ,2014, p.16)

Reconhecendo que a LGPD é uma política pública regulatória, ela realmente garantirá que se efetive a proteção dos dados pessoais de seus titulares? Por se tratar de uma lei recente, que regulamenta aspectos importantes da vida individual e em sociedade, mostrou-se oportuna e significativa entender o processo que levou a sua estruturação na forma da Lei nº 13.709 de 2018, e ainda mais especificamente observando-se a inserção do princípio da não discriminação nesta política pública regulatória sobre o tema da proteção de dados pessoais.

Contudo, e apesar de termos normas recentes que garantem o tratamento adequado de dados pessoais, se torna ainda mais necessário verificarmos se o Poder Judiciário também está de fato atendendo diretrizes formuladas pela Autoridade Nacional de Proteção de Dados e se há de fato proteção judicial para que o princípio não discriminatório seja atendido, pois o uso cada vez mais frequente de inteligência artificial não impede que discriminações continuem a serem reproduzidas, bem como o fato de sistemas de inteligência artificial aprenderem com dados, não garante que seus resultados sejam livres de preconceito ou discriminação. Os dados usados para treinar e testar tais sistemas, e a maneira como são projetados e usados, são todos

fatores que podem levar as pessoas a serem tratadas de forma menos favorável, ou colocadas em situações de desvantagem.

Em face do exposto, esta pesquisa segue a abordagem de pesquisa qualitativa, com uma técnica descritiva e tem como objetivo verificar como se deu o processo de construção do *princípio da não discriminação* na Lei Geral de Proteção de Dados Pessoais Brasileira por meio da análise dos aspectos jurídicos, projetos de lei, artigos acadêmicos e exemplos de situações vivenciadas de discriminações, bem como, observar a sua aplicabilidade nas decisões judiciais de 1ª Instância do Tribunal de Justiça do Estado de São Paulo, que mencionam referido princípio para assim verificar se há de fato esforços no Poder Judiciário para diminuir o número de dados pessoais colhidos de forma discriminatória. Pretende-se com este trabalho contribuir para a formulação e implementação de novas políticas públicas direcionadas a este tema, assim como auxiliar na adequação do Brasil à demanda mundial de proteção aos dados pessoais de todos os indivíduos.

Com o intuito de adentrar na pesquisa acima exposta, este trabalho está estruturado em 4 capítulos. O primeiro será a contextualização dos pressupostos e fundamentos que contribuíram para a inserção do princípio da não discriminação tanto na LGPD como na GDPR, já que traçar um panorama que demonstra a existência da discriminação relacionada ao tratamento dos dados pessoais valida a necessidade de se ter uma política pública regulatória que atenda aos anseios da sociedade. No segundo capítulo serão examinados os casos de discriminações, ocorrências e resultados obtidos e noticiados pela mídia, que tiveram por base a lei brasileira, como por exemplo nos casos envolvendo reconhecimento facial, *score* de crédito, processos seletivos de acesso a vagas de empregos, entre outros. No terceiro capítulo pretende-se examinar e analisar a atuação do Poder Judiciário, e mais especificamente as decisões judiciais de primeira instância do Estado de São Paulo, onde consta menção ao princípio da não discriminação, para verificarmos se de fato referido princípio está sendo atendido no âmbito jurídico. E no último e quarto capítulo será aprofundado o conceito de política pública para podermos a partir dai verificar a mobilização do Direito, sendo analisadas as limitações e as potencialidades da aplicabilidade deste conceito à realidade brasileira

# CAPÍTULO 1 – PERSPECTIVAS PARA ENFRENTAMENTO DE UM DESAFIO COLETIVO NA CONTEMPORANEIDADE: O PRINCÍPIO DA NÃO DISCRIMINAÇÃO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

## 1.1 – Contextualização sociocultural e necessidade de inserção da não discriminação na LGPD

> Os indivíduos tornam-se *dividuais*, divisíveis, e as massas tornaram-se amostras, dados mercados ou *bancos.*
> *Post-scriptum sobre as sociedades de controle.*
> Gilles Deleuze

O Brasil é um dos países mais desiguais do mundo se considerarmos as diversas áreas de análise tais como economia, educação e cultura, o que demonstra um desequilíbrio nas relações entre Estado e sociedade. E ao mesmo tempo, somos um dos países que mais compram e implementam novas tecnologias, e que tem direcionado a sua economia à análise de informações e mais especificamente ao colhimento de dados pessoais.

Neste sentido, o sociólogo Sérgio Amadeu da Silveira explica que "o processamento e mineração de informações envolve a agregação dos dados coletados e armazenados pelas tecnologias digitais, enriquecendo o perfil pessoal de cada indivíduo de maneira detalhada" (SILVEIRA, 2019). Estes perfis e coletas criam enormes oportunidades para novos produtos e serviços. A economia e a política se desenvolvem tendo por base o volume de informações e de dados que possuem, e por isso o conhecimento destes tornou-se, hoje muito mais do que no passado, um dos principais fatores que podem colaborar para a diminuição de desigualdades, ou não.

> No atual contexto, a nova configuração social em andamento está sendo chamada de Sociedade da Informação, resultante da convergência da base tecnológica que possibilitou a representação da informação em forma digital, da dinâmica da indústria e do crescimento da internet (TAKAHASHI, 2000).

Nas sociedades da informação, uma série de operações e decisões têm sido delegadas a algoritmos: escolhas essas que, em um passado não tão distante, sequer se cogitava a possibilidade de serem realizadas por outros que não os próprios seres humanos. "Esses algoritmos têm a capacidade de aconselhamento, quando não de pronta decisão, sobre a forma com que as informações e dados deverão ser interpretados, além de poderem definir ações a serem tomadas como resultado" (SCHREIBER; MARTINS; CARPENA, p. 21, 2022).

Inserida neste cenário, a LGPD, inspirada pelo Regulamento Europeu, possui como um de seus objetivos implementar mecanismos antidiscriminatórios na privacidade e proteção de dados pessoais. E estes mecanismos podem ser encontrados em diversos artigos da referida lei, pois positivam o princípio da não discriminação em seu artigo 6º, inciso IX, e também no artigo 5º, II, nos apresenta quais dados são sensíveis como forma de proteger ainda mais as pessoas consideradas vulneráveis, assim como no artigo 2º, o da autodeterminação informativa, o direito à privacidade, os direitos humanos, o livre desenvolvimento da personalidade e a dignidade e o exercício da cidadania pelas pessoas naturais, e em seu artigo 20, concretiza o direito de o titular de dados solicitar a revisão de decisões automatizadas.

Isso posto, fica explícito que a LGPD traz em seu ordenamento princípios que são essenciais para que haja de fato a proteção de dados pessoais tão necessários à sociedade contemporânea da chamada Sociedade da Informação ou da Era Digital, pois sabemos que o colhimento de dados pessoais visa, primeiramente, atender a interesses econômicos. Como nos diz Shoshana Zuboff ao utilizar como referência Max Weber – para quem os fins econômicos estão sempre imbuídos no desenvolvimento e na implantação da tecnologia –, as tecnologias digitais não são fins em si mesmas, afinal são subjugadas pela orientação lógica própria da forma econômica adotada em nossos tempos: o capitalismo de vigilância (ZUBOFF , p.33, 2021).

No entanto, o "descuido" no manejo dos dados pessoais por órgãos públicos e empresas privadas, contribui para que haja urgência no atendimento aos mecanismos antidiscriminatórios da LGPD, pois conforme nos alertou Linnet Taylor, em capítulo traduzido e intitulado "O que é justiça de dados? Conectando direitos digitais e liberdades globalmente", que consta no e-book "Construindo caminhos para a justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais":

> A crescente disponibilidade de dados digitais que refletem o desenvolvimento econômico e humano, em particular a chamada "fumaça dos dados" ou data fumes (Thatcher, 2014) – isto é, dados produzidos como subproduto da utilização de dispositivos e serviços tecnológicos – está provocando uma mudança de paradigma na elaboração de políticas públicas, que deixam de ser informadas por dados *(data informed*) para se tornarem orientadas por dados *(data driven*) (Kitchin, 2016). Essas fontes granulares de dados, que permitem a pesquisadores inferir os movimentos, atividades e comportamento das pessoas apresentam implicações éticas, políticas e práticas para a forma como as pessoas são vistas e tratadas pelo Estado e pelo setor privado (ou ambos agindo conjuntamente).
> Esta visibilidade distribuída tem implicações sociais e políticas ainda mais claras no caso de populações de baixa renda, sobre as quais a capacidade das autoridades públicas de coletar e reunir dados estatísticos costumava ser limitada. No entanto, a revolução dos dados é até agora primariamente técnica: o poder dos dados para

> classificar, categorizar e intervir ainda não foi explicitamente vinculado a uma agenda de justiça social pelas agências e autoridades que coletam, geram e utilizam dados. Tampouco existe um nível de conscientização elevado entre agentes de políticas públicas sobre como as novas tecnologias orientadas por dados podem não ser neutras em termos de acesso, utilização ou impactos, conforme demonstram pesquisas sobre este fenômeno (Dalton et al., 2016). Na realidade, enquanto a discriminação orientada por dados avança em um ritmo semelhante ao de tecnologias de processamento de dados, a conscientização e os mecanismos para combatê-la não. (BIONI, p.16, 2022)

A Lei Geral de Proteção de Dados Pessoais, ao inserir o princípio da não discriminação em seu artigo 6º, evidencia a intenção de sanar as desigualdades estruturais e institucionais, pois traz como desafio alcançar a justiça social quando propõe a democratização do acesso às intenções, ou melhor, à finalidade por quais nossos dados estão sendo tratados tanto em ambientes privados como públicos. E ter acesso a essas informações, até então restritas nas mãos das grandes corporações, faz com que haja um equilíbrio entre as relações de poder, o que contribuirá para que de fato estejamos mais próximos do fortalecimento do Estado Democrático de Direito.

Monique Mann e Tobias Matzner, em artigo intitulado "Perfil algorítmico desafiador: os limites da proteção de dados e antidiscriminação em resposta à discriminação emergente", mostram que um dos instrumentos mais utilizados na contemporaneidade para discriminar pessoas se chama "perfil algorítmico", e através dele é feita uma classificação social, vejamos:

> O perfil algorítmico pode resultar em classificação social e outros resultados discriminatórios (ver, por exemplo, Lyon, 2003, 2014; Parsons, 2015). Pesquisas na Austrália (Mann e Daly, 2019) e na América do Norte (Browne, 2015; Eubanks, 2018; Noble, 2018; Peña Gangadharan, 2012; Sandvig et al., 2016) demonstram como o perfil algorítmico tem como alvo grupos marginalizados, como minorias raciais, indivíduos de baixo nível socioeconômico e mulheres. Browne (2015) argumenta que o perfil algorítmico perpetua hierarquias baseadas no emaranhado de características de identidade. As práticas discriminatórias tornam-se autoaplicáveis com ciclos de feedback, à medida que são construídos conjuntos de dados que contêm dados desproporcionalmente sobre certas pessoas, levando ao supermonitoramento e superpoliciamento desses grupos (ver, por exemplo, Ferguson, 2017). É importante ressaltar que os efeitos discriminatórios também ocorrem se os dados sobre características discriminatórias, como sexo, raça, etnia etc., não forem processados diretamente.

O termo *discriminação* refere-se tanto ao ato de separação lícita, podendo ser incluído não só pessoas, mas objetos também, quanto ao ato de separação ilícita que envolve o tratamento injusto de pessoas. Em que pese a existência desse significado neutro de mera separação, quando se fala em discriminação, atualmente o significado mais utilizado é o do

tratamento diferenciado de pessoas, especificamente aquele considerado ilícito. Assim, vejamos:

> DISCRIMINAÇÃO s.f. (lat. discriminatio,onis) 1. Capacidade de discriminar; discernimento. 2. Ação de segregar, pôr à parte. 3. P.ext. Modo injusto de tratar alguém por causa de características pessoais; preconceito. DISCRIMINAR [Conj. 4] v.t. (lat. discriminare) 1. Distinguir as diferenças; discernir 2. Separar, especificar, listar. 3. P.ext. Tratar injustamente alguém por causa de alguma característica pessoal, classe social, religião, etc. v.t. e pr. 4. Separar(-se) de determinada(s) pessoa(s), formando grupo à parte, por razões étnicas, culturais etc.; apartar(-se).(LAROUSSE, 2006, p. 869)

E "a discriminação proibida, contudo, não será apenas aquela baseada em características pessoais, mas também as que se baseiem em fatos cuja adoção, uma vez tomados como critério de diferenciação, tenham por consequência prejuízo ao seu titular, como pode ocorrer em relação ao exercício regular de um direito" (art. 21 da Lei Geral de Proteção de Dados) (JUNQUEIRA, 2020). Nesse sentido, o que se combate na LGPD é a discriminação que utiliza dados pessoais de forma ilícita e abusiva.

Sendo assim, a LGPD proíbe a discriminação negativa e autoriza a positiva (lícita). Nesse sentido, Caitlin Mulholland traz como lição a seguinte análise:

> Em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. O legislador, ao relacionar o uso discriminatório às qualidades de ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo. Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. Assim, por exemplo, seria legítimo a um operador de dados que esteja realizando a precificação de um serviço de seguros de automóveis, tratar de maneira diferenciada os dados de mulheres entre 35 e 45 anos e mães, com a finalidade de oferecimento de um valor que reflita os riscos de danos usualmente ocasionados ou sofridos por esse grupo determinado de pessoas. Ou seja, há a possibilidade de tratamentos discriminatórios de dados, desde que não se caracterizem pela ilicitude ou abusividade, o que será determinado segundo critérios definidos tanto pelas regras expressas de direito civil e penal, quanto por princípios como o da boa-fé objetiva (MULHOLLAND , p. 164-165, 2018).

Contudo, no Brasil o que se constata é que, com o uso desenfreado de dados pessoais, são gerados efeitos discriminatórios graves, como no caso de pessoas que foram presas devido à falha do sistema utilizado pela segurança pública de reconhecimento facial, ou então, quando a geolocalização do celular indica o lugar da residência do titular de dados sem que este saiba, fazendo com que ele não seja considerado apto a preencher uma vaga de emprego. Ou seja,

> Uma variedade de características interligadas – raça, etnia, religião, gênero, localização, nacionalidade, status socioeconômico – determinam como indivíduos se tornam sujeitos de direito por meio do uso de seus dados e, consequentemente, como estes dados podem ser empregados por agentes decisórios, empresas ou ambos para definir ações que os impactam. Por sua vez, a possibilidade de uma pessoa ser identificada como alvo de vigilância multiplica-se dependendo do número de categorias de interesse a que ele pertença (TAYLOR , 2022).

A falta de controle sobre como os dados pessoais são tratados traz implicações sociais e políticas ainda mais claras no caso de populações de baixa renda, sobre as quais a capacidade das autoridades públicas de coletar e reunir dados estatísticos costumava ser limitada. “No entanto, a revolução dos dados é até agora primariamente *técnica*: o poder dos dados para classificar, categorizar e intervir ainda não foi explicitamente vinculado a uma agenda de justiça social pelas agências e autoridades que coletam, geram e utilizam dados” (TAYLOR , 2022).

Por isso, as proteções antidiscriminação em contextos de processamento de dados contemporâneos (e futuros) também podem ter aplicação limitada, devido às dificuldades em identificar tratamento diferenciado com base em motivos protegidos, especialmente quando são abstratos, interseccionais ou emergentes – uma crítica que estendemos abaixo, diagnosticando problemas de aplicação de salvaguardas antidiscriminação e propondo maneiras de corrigi-los para torná-los adequados para lidar com as formas complicadas de discriminação que surgem na criação de perfis algorítmicos (JUNQUEIRA, 2020).

A discriminação refere-se à ação de tratar alguém de forma injusta ou desigual com base em características como raça, gênero, religião, orientação sexual, entre outros. A discriminação pode ocorrer em várias esferas da vida, como no trabalho, na educação, no acesso a serviços públicos e em situações cotidianas. É um fenômeno social complexo que pode levar à marginalização e à violação dos direitos humanos.

Desta forma, podemos concluir que o Brasil precisa manter-se vigilante em relação ao atendimento do princípio da não discriminação como forma de estarmos inseridos de forma mais democrática aos anseios do mundo contemporâneo, que se apoia no colhimento de dados pessoais para se desenvolver tanto no âmbito privado como no público. Adiante, será desenvolvida uma discussão mais aprofundada acerca do conceito da discriminação e dos motivos que levaram a sua inserção no ordenamento jurídico brasileiro.

## 1.2 – Panorama do princípio da não discriminação nas leis nacionais e internacionais

A Lei Geral de Proteção de Dados Pessoais consolida em um só documento outras leis anteriores que abordavam de forma específica sobre a privacidade e proteção de dados pessoais, tais como a Lei 9029/95 que proíbe práticas discriminatórias para efeitos admissionais ou de permanência, Lei 7716/89 Lei da Antidiscriminação por Raça, Cor e Etnia, Lei 8213/91 Lei da Previdência, Lei 10471/2003 Estatuto do Idoso, Convenção OIT 098 que aplica os princípios do Direito de Organização e de Negociação Coletiva , Convenção OIT 111 que trata sobre a Discriminação em matéria de emprego e profissão, Lei 13146/2015 Lei Brasileira de Inclusão da pessoa com Deficiência, Convenção OIT 103 de Amparo à Maternidade, LC 150/2015 Lei das Domésticas, Convenção OIT 100 de Igualdade de Remuneração para a mão-de-obra feminina por um trabalho de igual valor, NR/5 MTE Comissão Interna de Prevenção de Acidentes CIPA e a Lei 11788/08 Lei do Estágio.

A LGPD, em um só documento harmoniza e complementa leis que de alguma forma e em diferentes momentos tratam de assuntos relacionados a dados e no caso de grande parte das leis apontadas acima também trazem como tema a discriminação seja ela lícita, ilícita ou abusiva.

Das Leis apontadas acima, a primeira delas a 9029/95, que proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências[1] veda especificamente a exigência de 1 (um) documento (atestado médico) e de 1 (um) exigir (esterilização) mostrando neste trecho o caráter taxativo, uma vez que apontam diretamente condutas que não podem ser tomadas e também “resguardam interesses fundamentais da sociedade e por isso obrigam independente da vontade das partes”[2].

A importância dessa lei reside no fato de que ela visa garantir a igualdade de oportunidades no ambiente de trabalho, impedindo a discriminação baseada em questões de gênero e saúde reprodutiva e, ao proibir a exigência de atestados de gravidez, a lei protege as mulheres contra possíveis demissões ou preconceitos durante o processo de seleção, assegurando que a maternidade não seja um critério de exclusão profissional.

Contudo, quando referida Lei veda “outras práticas discriminatórias” ela se apropria de um conceito aberto para proibir qualquer outra prática discriminatória no ambiente de trabalho além daquelas 2 (duas) taxativas.

---

[1] Site: https://www.planalto.gov.br/ccivil_03/leis/l9029.htm acesso em 25 de junho de 2023

[2] DINIZ, Maria Helena – Compêndio de Introdução à Ciência do Direito – 6ª ed. Atual – São Paulo: Saraiva, 1994, p.65

Importante dizer que uma norma de conceito fechado é aquela que estabelece de forma clara e precisa o seu alcance e aplicação. Ela define detalhadamente as condições, critérios e elementos necessários para que determinada conduta seja considerada ilícita ou legítima. Essas normas oferecem pouca margem para interpretação subjetiva, uma vez que sua redação é específica e delimitada. São exemplos de normas de conceito fechado as que estabelecem limites de velocidade em uma estrada ou definem a idade mínima para a aquisição de bebidas alcoólicas.

Já uma norma de conceito aberto é aquela que possui termos e conceitos mais amplos e abrangentes, deixando espaço para interpretação e aplicação de acordo com o contexto e os princípios envolvidos. Essas normas são mais flexíveis e permitem que o intérprete, seja o juiz ou autoridade responsável pela aplicação da lei, utilize seu conhecimento, experiência e bom senso para decidir casos específicos. São exemplos de normas de conceito aberto aquelas que estabelecem o dever de agir com "boa-fé", "razoabilidade" ou "proporcionalidade", termos que requerem análise contextual e subjetiva (LARENZ , 1997).

Em resumo, uma norma de conceito fechado é mais restritiva, determinando com precisão as situações a que se aplica, enquanto uma norma de conceito aberto é mais flexível, permitindo uma margem maior de interpretação de acordo com os princípios e valores envolvidos. Ambos os tipos de normas desempenham um papel importante na legislação, cada um com suas características e propósitos específicos.

Já a Lei nº 7.716, de 5 de Janeiro de 1989, que define os crimes resultantes de preconceito de raça ou de cor[3], principalmente em seu artigo 20-C que estabelece que na interpretação desta Lei, o juiz deve considerar como discriminatória qualquer atitude ou tratamento dado à pessoa ou a grupos minoritários que cause constrangimento, humilhação, vergonha, medo ou exposição indevida, e que usualmente não se dispensaria a outros grupos em razão da cor, etnia, religião ou procedência.[4] Esta lei adota um conceito mais fechado uma vez que descreve uma conduta criminosa mais específica e por isso podemos dizer que ela seja mais assertiva e objetiva, ao contrário da Lei objeto deste estudo que, ao estabelecer o princípio da não discriminação em seu ordenamento, estabelece um parâmetro somente com relação à abusividade e ilicitude da conduta, sem taxar ou exemplificar situações em que de fato o ato

[3] Site do Planalto: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm#:~:text=LEI%20N%C2%BA%207.716%2C%20DE%205%20DE%20JANEIRO%20DE%201989.&text=Define%20os%20crimes%20resultantes%20de,de%20ra%C3%A7a%20ou%20de%20cor.&text=Art.%202%C2%BA%20 , acesso em 25 de junho de 2023.
[4] Idem.

discriminatório segundo a LGPD poderá ser caracterizado. Por isso podemos dizer que a LGPD é a soma de todas as outras leis que descreveram em diferentes momentos e situações quais seriam as condutas discriminatórias que podem ser incluídas no princípio da não-discriminação.

Entretanto, a LGPD que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[5], estabelece a forma como os dados pessoais são tratados para que se possa definir se tal dado pode ou não discriminar uma pessoa. E para que este princípio seja de fato atendido precisamos além de compreendermos o que é entendido como discriminação nas leis apontadas acima, devemos entender qual a arquitetura do conjunto de dados, ou seja, as estruturas de dados relacionadas, diversos sistemas de informação, bem como, não devemos nos atermos somente à letra da lei, mas também à hermenêutica que está inserida no princípio em epígrafe.

Dessa maneira, é também preciso revisitarmos conceitos que definem o que são princípios, e como eles foram conceituados por grandes juristas brasileiros. Sendo assim, começamos com Miguel Reale, que nos diz:

> Princípios são, pois verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade. Às vezes também se denominam princípios certas proposições, que apesar de não serem evidentes ou resultantes de evidências, são assumidas como fundantes da validez de um sistema particular de conhecimentos, como seus pressupostos necessários (REALE, 1986).

Para Luis Roberto Barroso, princípios

> são o conjunto de normas que espelham a ideologia da Constituição, seus postulados básicos e seus fins. Dito de forma sumária, os princípios constitucionais são as normas eleitas pelo constituinte como fundamentos ou qualificações essenciais da ordem jurídica que institui (BARROSO, 1999).

Por fim, Celso Antônio Bandeira de Mello, sobre os efeitos de sua inobservância:

> Princípio – já averbamos alhures – é, por definição, mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e servindo de critério para sua exata compreensão e inteligência, exatamente por definir a lógica e a racionalização do sistema normativo, no que lhe confere a tônica e lhe dá sentido harmônico. É o

[5] Artigo 1º da Lei 13709 de 2018. Site:https://www.planalto.gov.br/ccivil_03/_ato2015018/2018/lei/l13709.htm. Acesso em 25 de junho de 2023.

> conhecimento dos princípios que preside a intelecção das diferentes partes componentes do todo unitário que há por nome sistema jurídico positivo [...]. Violar um princípio é muito mais grave que transgredir uma norma qualquer. A desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo o sistema de comandos. É a mais grave forma de ilegalidade ou de inconstitucionalidade, conforme o escalão do princípio atingido, porque representa insurgência contra todo o sistema, subversão de seus valores fundamentais, contumélia irremissível a seu arcabouço lógico e corrosão de sua estrutura mestra. Isto porque, com ofendê-lo, abatem-se as vigas que os sustêm e alui-se toda a estrutura nelas esforçada (MELLO, 2000).

Estes conceitos nos mostram que os princípios carregam consigo alto grau de imperatividade, o que denota o seu caráter normativo, cogente, impositivo de observância obrigatória. E o não atendimento a eles pode acarretar a ilegalidade e a inconstitucionalidade do ato do poder público, trazendo consequências desastrosas para a sociedade como um todo.

Logo, é importante observar também o contexto que impulsionou a criação da LGPD, uma vez que se torna de extrema relevância analisar os motivos que contribuíram para a inserção do princípio da não discriminação.

Desde o final do século XX, vem sendo observada e debatida a necessidade da privacidade e da proteção dos dados pessoais, porém somente no ano 2000 é que esta discussão ganhou fôlego:

> Então apenas uma semente, essa ideia só ganharam maior tração a partir de meados dos anos 2000, com a participação do Brasil em negociações internas do Mercosul, foro que abrigou movimentos de pressão, por parte de países como a Argentina, para a construção de uma norma comum aos países do bloco. Embora nunca se tenha concretizado a ideia de uma regulação de proteção de dados para todos os países integrantes do Mercosul, os debates deflagrados por essa proposta serviram de combustível para a internalização do tema pelo Poder Executivo brasileiro (BIONI; RIELLI, 2021).

Em 2010, diversos grupos representativos da sociedade civil, empresas de diferentes ramos, pesquisadores, organizações não governamentais e órgãos públicos, entre eles representativos dos consumidores, como Procons, contribuíram para as discussões que levaram à sua elaboração, revisão e consequente aprovação em agosto de 2018, o que deu um caráter multiparticipativo à LGPD.

Por isso, podemos dizer que ela é resultado das exigências mais atuais da contemporaneidade, dada a utilização de técnicas de *big datas, machine learning* e inteligência artificial, que estão cada vez mais presentes nos governos e órgãos públicos. E assim, se torna cada vez mais comum a coleta de vários tipos de dados, inclusive biométricos, estando entre eles os de DNA, tipo de sangue, impressões digitais, gravações de voz e imagem. Em razão deste cenário, as políticas públicas regulatórias se tornaram importantes para proteger a

privacidade, a transparência, e para contribuir com a diminuição de discriminações que podem estar presentes na forma como os dados são tratados, tanto por instituições públicas como pelas privadas, garantindo a proteção aos direitos fundamentais da privacidade e da liberdade, tal como inserido recentemente no artigo 5º da Constituição Federal.

> Com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD), passamos a contar com um marco normativo indispensável à nossa integração à economia digital. Já contávamos, por certo, com normas protetivas de grande alcance. Na Constituição Federal já se asseguravam os direitos à intimidade, à vida privada e ao sigilo de dados e prevê o habeas data. No Código de Defesa do Consumidor (Lei nº 8.078/1990) foram enunciados importantes direitos relativos a cadastros de consumidores, como os de acesso, comunicação, correção e limitação temporal, que prefiguraram alguns dos princípios caros às legislações de proteção de dados pessoais. Na Lei do Cadastro Positivo (Lei nº 12.414/2011), na Lei de Acesso à Informação (Lei nº 12.527/2011) e no Marco Civil da Internet (Lei nº 12.965/2014), já se identificavam importantes contribuições à proteção de dados pessoais. Mas a LGPD é a primeira lei no Brasil a tratar de modo sistemático e coerente a proteção de dados pessoais, definindo regras e procedimentos estruturantes dessa nascente área do direito, o que terá grande impacto na vida das pessoas, das empresas e dos entes dos setores público e privado, de modo geral (BIONI, 2021).

Contudo, a LGPD teve a sua total vigência iniciada em 18 de setembro de 2020, e estabelece em seu artigo 1º a proteção de dados pessoais em diversos ambientes, público ou privado, que objetiva proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Porém, especificamente com relação ao tratamento de dados em ambiente público, esta mesma lei prevê que:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> (...)
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

Vemos também que a Constituição Federal em seu artigo 5º, garante respeito à intimidade, à vida privada, à honra e à imagem das pessoas. Tal garantia é, também, observada em diferentes marcos legislatórios como o próprio Marco Civil da Internet (Lei 12.965/2014) e a Lei de Acesso à Informação (Lei 12.527/2011), entre outros.

Na área pública, e buscando estimular e facilitar o compartilhamento de dados na Administração Pública, foi sancionado o Decreto Lei 10.046, em 9/10/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da Administração Pública Federal e institui o Comitê Central de Governança de Dados e o Cadastro Base do Cidadão.

Mesmo acompanhada por diversos mecanismos legislativos que discorrem sobre assuntos comuns ao tema da privacidade e proteção de dados, a LGPD por si só já traz muitos desafios aos titulares de dados, aos poderes públicos e privados, à Autoridade Nacional de Proteção de Dados (ANPD) e aos operadores do Direito.

Destaca-se a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), criada pela Medida Provisória n. 869, de 27 de dezembro de 2018, na qual a conversão em lei foi aprovada pelo Senado Federal em maio de 2019, e cuja competência regulatória impõe uma série de medidas para que se proceda a normatização de técnicas e orientações para atendimento à LGPD. No dia 13 de junho de 2022, a Medida Provisória (MPV) nº 1.124, transformou a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial, dando a esta maior autonomia, independência, mais capacidade para priorizar ações em prol da sociedade e poder de influência para que a lei seja de fato atendida.

A LGPD concedeu à ANPD a responsabilidade por zelar pelos dados pessoais, com poderes de fiscalização, sanção e regulação tendo, portanto, um papel relevante e importante na construção de um arcabouço jurídico de proteção ao titular que viabiliza o uso adequado de dados pessoais em diferentes contextos públicos e privados (ANPD, 2022).

No entanto, apesar da existência da ANPD, a aplicação de sanções vem surgindo de forma tímida por esta. Contudo, o Judiciário através da provocação de órgãos públicos como o Ministério Público, Defensoria Pública e Procons está tomando à frente neste sentido, porque por mais que a ANPD tenha o papel de zelar pela proteção de dados pessoais, fiscalizar e aplicar sanções em caso de descumprimento à legislação, ela mais emite diretrizes, estabelece regras, do que fiscaliza ou sanciona aqueles que descumprem a LGPD.

Não só no Brasil como em um número significativo de países, os governos ao redor do globo perceberam a necessidade de regulamentação, controle e fiscalização das práticas e políticas antidiscriminatórias relacionadas aos dados pessoais.

> A Comissão da União Europeia foi a primeira a perceber a necessidade crescente de proteger seus cidadãos e garantir a eles seus direitos referentes à proteção de dados pessoais. O fez por meio do Regulamento Geral sobre a Proteção de Dados (GDPR, sigla em inglês) (COSTA, 2019, p. 2)

Importante dizer que a LGPD é fruto da GDPR, e que o princípio da discriminação foi nela incluído devido a vários fatores, mas o mais conhecido deles se refere à utilização incorreta de dados em um Hospital acusado de usar critérios misóginos e xenófobos na admissão de seus funcionários. Pois:

> Nas décadas de 1970 e 1980, o St. George's Hospital Medical School, no Reino Unido, utilizou um programa desenvolvido para realizar uma triagem inicial dos solicitantes. O programa, que imitava as escolhas que a equipe havia feito no passado, negou entrevistas a 60 candidatos, porque eram mulheres ou porque tinham nomes que não eram de origem europeia.(COSTA, 2019)

Se em 1970, na Europa, estudos comprovaram a utilização de dados pessoais para discriminar, a consequência disso no Brasil tem efeito devastador até os dias atuais. Pois a discriminação ainda está presente nas oportunidades de emprego, em questões de moradia, segurança, saúde, crédito e consumo.

Após a publicação da GDPR, foi a vez do Estado Norte-Americano da Califórnia e do Brasil de redigirem suas Leis Gerais de Proteção de Dados (STATE OF CALIFORNIA, 2018). No Brasil, o Marco Civil da Internet foi a reação primária à necessidade de regulamentação da privacidade e proteção de dados pessoais. Embora genérico, constituiu uma base para futuros debates e regulamentações sobre o tema, como abaixo se lê:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> (...)
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei[6];
> (...)

Apesar destas legislações já existirem, ainda aguardamos orientações da Autoridade Nacional de Proteção de Dados para que ocorra o adequado atendimento ao referido princípio. As orientações que serão publicadas, contribuirão na formulação e implementação de políticas públicas que estarão inseridas neste novo cenário de proteção e privacidade de dados pessoais e que certamente contribuirão para a diminuição de desigualdades de tratamento discriminatório.

Porém, enquanto a ANPD caminha a passos lentos, até o ano de 2021, 598 decisões judiciais trataram sobre a proteção de dados pessoais e da privacidade, sendo que em pesquisa realizada pela empresa *Juit*, identificou-se que 74% das sentenças são de primeiro grau e estão restritas a São Paulo[7].

Desta forma, ao direcionarmos o nosso olhar para o princípio antidiscriminatório que garante o tratamento adequado e igualitário de dados pessoais, devemos nos atentar e verificar se a Autoridade Nacional de Proteção de Dados (ANPD), bem como o Judiciário, estão criando

---

[6] Site http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em 12/04/23

[7] LGPD: Justiça já possui 600 decisões envolvendo a lei. In: https://www.tecmundo.com.br/seguranca/220496-lgpd-justica-possui-600-decisoes-envolvendo-lei.htm Acesso em 05.11.22

meios adequados e diretrizes para que de fato este seja atendido pelo poder público e também privado, tanto nos ambientes físicos como também nos virtuais.

Por fim, esta pesquisa apresentará no próximo capítulo a movimentação do Poder Judiciário com relação ao atendimento ao princípio da não discriminação, prevista na LGPD, já que falta a elaboração de regulamentações pela ANPD direcionadas e específicas ao referido princípio. Desta forma, serão demonstradas quais medidas judiciais aplicadas pelo Tribunal de Justiça do Estado de São Paulo existem para coibir as discriminações negativas provenientes do tratamento de dados pessoais de forma abusiva e ilícita.

## 2. DISCRIMINAÇÕES BASEADAS NO USO DE DADOS PESSOAIS

"Os privilegiados são analisados por pessoas; as massas, por máquinas"
Cathy O´Neal

A própria essência da economia de dados pessoais é que todos somos tratados de forma diferente, de acordo com os nossos dados. É justamente porque somos tratados de maneira diferente que os algoritmos acabam sendo sexistas e racistas. É porque somos tratados de forma diferente por causa dos nossos dados que pessoas diferentes podem pagar preços diferentes pelo mesmo produto sem saber que podem estar pagando mais do que os outros. É porque somos tratados de maneira diferente que podemos ver conteúdos diferentes, o que amplifica ainda mais nossas diferenças – um ciclo vicioso de diferenciação e desigualdade. Não importa quem você seja, você deve ter o mesmo acesso a informações e oportunidades. As personificações da justiça são frequentemente retratadas usando uma venda, simbolizando a imparcialidade da justiça. A privacidade é o que pode cegar o sistema para garantir que sejamos tratados de forma igualitária e imparcial. A privacidade é a venda da justiça. (VÉLIZ, p. 124, 2021)

O mundo vive uma revolução tecnológica sem precedentes, impulsionada pelo crescimento exponencial da internet e das tecnologias digitais. Nesse contexto, o conceito de "Capitalismo de Vigilância", trazido por Shoshana Zuboff no livro a Era do Capitalismo de Vigilância, emerge como uma poderosa força que molda a economia e a sociedade contemporânea. Essa abordagem econômica se baseia na coleta massiva de dados pessoais dos usuários para alimentar o lucro e o poder das grandes empresas, gerando debates necessários sobre privacidade, ética e o futuro da democracia.

O Capitalismo de Vigilância está enraizado na ideia de que os dados pessoais são um recurso extremamente valioso, pois permitem o mapeamento detalhado dos comportamentos, preferências e hábitos dos indivíduos. As gigantes da tecnologia, plataformas digitais e outras empresas, cada vez mais, adotam modelos de negócios baseados na coleta, análise e comercialização desses dados. Esse processo envolve o rastreamento constante das atividades online e offline dos usuários, desde suas pesquisas na internet até suas interações em redes sociais e movimentos físicos por meio de dispositivos móveis.

Por isso, as implicações do Capitalismo de Vigilância são profundas e variadas. Em primeiro lugar, a coleta indiscriminada de dados pessoais pode comprometer a privacidade dos indivíduos, expondo informações íntimas e sensíveis sem o seu conhecimento ou consentimento adequado. A noção de anonimato na era digital torna-se cada vez mais tênue, uma vez que a quantidade de dados coletados permite a identificação precisa de usuários.

Em segundo lugar, o acúmulo de informações detalhadas sobre os indivíduos permite que as empresas personalizem produtos, serviços e anúncios de forma altamente direcionada, maximizando o engajamento e, consequentemente, os lucros. Entretanto, essa prática levanta questões éticas sobre a manipulação comportamental e a exploração psicológica dos usuários, além de criar bolhas de informação que podem reforçar visões de mundo estreitas.

Em terceiro lugar, o poder concentrado nas mãos das empresas de tecnologia levanta preocupações sobre monopólios e oligopólios que controlam a esfera digital. A acumulação de dados e a posição dominante dessas empresas podem restringir a competição e inovação, limitando a diversidade de ideias e serviços disponíveis aos consumidores.

Além disso, o Capitalismo de Vigilância também pode ter implicações políticas substanciais. A coleta e análise de dados podem ser usadas para influenciar eleições, disseminar desinformação e manipular o discurso público, minando as possibilidades de alcançarmos de fato o Estado Democrático de Direito, por isto ele deve ser visto como um fenômeno complexo que desafia as bases éticas, políticas e sociais da era digital. É crucial, que seja encontrado um equilíbrio entre o avanço tecnológico e a proteção dos direitos individuais, a fim de construir uma sociedade digital mais justa, segura e responsável. Somente com uma abordagem coletiva e consciente poderemos enfrentar os desafios impostos pelo poder dos dados na era da vigilância.

Desta maneira, a relação entre o Capitalismo de Vigilância, proteção de dados e discriminação é intrincada e de extrema importância para o futuro da sociedade digital. Ao abraçar um modelo de negócio centrado na coleta massiva de dados pessoais, as empresas

podem acabar perpetuando vieses e discriminações existentes na sociedade. A análise de informações sensíveis pode levar à criação de perfis estereotipados, resultando em práticas discriminatórias em áreas como emprego, habitação e acesso a serviços. A ausência de regulamentação rigorosa e de práticas éticas pode agravar ainda mais essa problemática, comprometendo a privacidade e os direitos individuais, além de reforçar desigualdades sociais.

Portanto, é imperativo que a proteção de dados seja uma prioridade na era do Capitalismo de Vigilância. A implementação de leis e regulamentos robustos, como a LGPD e o GDPR, é essencial para garantir que as empresas tratem os dados pessoais com responsabilidade e transparência. Além disso, a conscientização e a educação sobre a importância da privacidade digital devem ser amplamente difundidas, capacitando os usuários a protegerem suas informações e compreenderem os riscos associados ao compartilhamento de dados. Somente por meio de um esforço coletivo de governos, empresas e indivíduos podemos enfrentar os desafios da discriminação no Capitalismo de Vigilância e construir uma sociedade digital inclusiva, ética e justa.

Tendo como ponto de entendimento de que a privacidade dos dados pessoais é condição primordial para que os casos de injustiça diminuam, esta pesquisa trará neste capítulo temas recentes que relacionam o uso da tecnologia às discriminações causadas no uso de reconhecimento facial, *score* de crédito e nos processos seletivos de acesso a vagas de empregos.

## 2.1 Reconhecimento facial

A tecnologia de reconhecimento facial pode ser descrita como um sistema que: funciona mediante o uso de identificação biométrica para mapear características faciais de uma pessoa presente em uma fotografia ou vídeo, comparando as informações obtidas com um banco de rostos conhecidos para encontrar uma correspondência (OLIVEIRA, pg. 15, 2021).

A biometria se destaca como uma tecnologia que, embora promissora, também suscita preocupações significativas quanto à privacidade e à segurança dos cidadãos.

Inserida no rol de dados sensíveis que são informações que, quando mal utilizadas ou expostas, podem causar danos emocionais, financeiros ou sociais aos titulares. Eles incluem dados de origem racial ou étnica, opiniões políticas, crenças religiosas, informações genéticas, dados biométricos, entre outros; dentre esses, a biometria é um conjunto de técnicas que visa

identificar, medir e analisar características físicas e comportamentais únicas de uma pessoa, como impressões digitais, reconhecimento facial, íris, voz, entre outras.

A adoção da biometria trouxe inúmeras vantagens em diversos setores, desde o acesso mais seguro a dispositivos e sistemas até a prevenção de fraudes e crimes. No entanto, é importante ponderar os riscos associados ao uso dessa tecnologia, por se tratar de dados sensíveis. A coleta e armazenamento inadequado de informações biométricas podem resultar em consequências graves, como o vazamento de dados pessoais, a identidade digital comprometida e o risco de falsificação.

Além disso, questões éticas emergem à medida que as tecnologias biométricas são amplamente utilizadas. É crucial garantir a transparência e o consentimento informado dos indivíduos antes da coleta e processamento de suas informações biométricas. Afinal, a biometria envolve a captura de detalhes altamente íntimos e, portanto, exige a construção de um ambiente confiável, em que os cidadãos se sintam protegidos e empoderados em relação ao uso de suas informações pessoais.

Em termos regulatórios, a proteção de dados sensíveis, incluindo informações biométricas, é um tema central para a legislação de privacidade e segurança de dados em diversos países. Leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia têm como objetivo resguardar a privacidade dos cidadãos e impor responsabilidades às organizações que tratam dados sensíveis.

Por outro lado, é importante destacar que a biometria também oferece oportunidades significativas no contexto de proteção e segurança de dados. Uma vez implementadas de maneira responsável e alinhada às leis de proteção de dados, as tecnologias biométricas podem fortalecer a autenticação de usuários, diminuir a necessidade de senhas inseguras e, consequentemente, aumentar a proteção contra ataques cibernéticos.

A relação entre dados sensíveis e biometria é complexa e multifacetada. A tecnologia biométrica traz benefícios notáveis, mas requer uma abordagem cuidadosa para garantir a proteção da privacidade e dos direitos dos indivíduos. É essencial que governos, empresas e instituições adotem práticas éticas e seguras na coleta e utilização de dados biométricos, ao mesmo tempo em que proporcionam transparência e controle aos cidadãos sobre o tratamento de suas informações pessoais. Somente dessa forma poderemos aproveitar plenamente os benefícios da biometria enquanto protegemos os valores fundamentais da privacidade e da dignidade humana.

Assim, esse tipo de tecnologia pode ser aplicado não apenas à comprovação da identidade de um sujeito, como também — e supostamente — para evitar crimes referentes à identidade[8]; promover controle de acesso a espaços e serviços públicos e privados; reconhecer criminosos; gerar prova de vida (amplamente utilizada pelo governo brasileiro em aplicativos como, por exemplo, gov.br); desbloquear equipamentos etc. É importante salientar que as tecnologias biométricas não se resumem às tecnologias de reconhecimento facial — ao contrário: elas podem analisar as impressões digitais, a retina, a íris, a voz, o modo de andar, entre outros dados pessoais biométricos[9]. Em todos esses casos, os dispositivos processam métricas que seriam únicas e exclusivas de cada indivíduo para fins de identificação e reconhecimento.

E por estes motivos, a relação entre reconhecimento facial e proteção de dados pessoais é um tema de extrema relevância e que desperta preocupações éticas e jurídicas. E além do mais, o avanço da tecnologia e a crescente utilização de sistemas de reconhecimento facial levantam questionamentos sobre a privacidade e segurança das informações pessoais.

O reconhecimento facial é uma tecnologia que utiliza algoritmos para identificar e autenticar indivíduos com base em características faciais únicas e assim, é amplamente utilizado em diversos setores, desde o desbloqueio de smartphones até o controle de acesso em ambientes corporativos.

> Reconhecimento facial é uma técnica de identificação biométrica, assim como a impressão digital, em que um software mapeia as linhas faciais e, através de algoritmos, compara-os a uma imagem digital, reconhecendo (ou negando) sua identidade. (MAGNO; BEZERRA, 2009).

[8] O Código Penal em seus artigos 307 e 308 define os critérios-base para crime de falsa identidade, contudo não faz qualquer menção a características biométricas para caracterização de tal crime. As tecnologias de reconhecimento facial têm sido utilizadas também com a finalidade de validação de identidade e sistema antifraude por diversos órgãos públicos e privados, a exemplo do SPC, que lançou em 2019 um ferramenta que permite a verificação de lojas do varejo ao confirmar a identidade real de um consumidor a partir de imagens colhidas no momento em que o sujeito tem acesso a determinado crédito. O sistema compara essas imagens com outras que existem em suas bases de dados para, supostamente, informar ao lojista a verdadeira identidade de quem está consumindo ou acessando crédito. Todo o propósito do sistema seria garantir segurança ao consumidor, entretanto o que ele faz na verdade é conceder a lojistas poder de polícia. Para mais informações a esse respeito, ver: https://bit.ly/3t7ZOnm. Esse modo de validação da identidade tem sido amplamente utilizado por diversas instituições públicas e privadas, conforme apontam Mariah Rafaela Silva e Joana Varon em um estudo publicado em 2021 intitulado “Reconhecimento Facial no Setor Público”.

[9] Segundo o inciso II do artigo 2º do decreto que institui o Cadastro Base do Cidadão, “atributos biométricos” de interesse do Cadastro são “características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar”. Decreto n 10.046 de 9 de out. de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm . Acesso em: 10 mar. 2023.

Entretanto o acesso a dados sensíveis, como a biometria, contribui para que seja mantida ou até mesmo ampliada uma estrutura de poder que passa a ser empreendido no monitoramento das mínimas atitudes do indivíduo, o que foi denominado por Foucault de Microfísica do Poder, uma vez que:

> Forma-se uma política das coerções que são um trabalho sobre o corpo, uma manipulação calculada de seus elementos, de seus gestos, de seus comportamentos. O corpo humano entra numa maquinaria de poder que o esquadrinha, o desarticula e o recompõe. 'Uma anatomia política', que é também igualmente uma 'mecânica do poder', está nascendo, ela define como se pode ter domínio sobre o corpo dos outros, não simplesmente para que façam o que se quer, mas para que operem como se quer, com as técnicas, segundo a rapidez e a eficácia que se determina. (FOUCAULT, p. 119, 1987)

Assim, a coleta, armazenamento e utilização desses dados biométricos suscitam preocupações relacionadas à proteção da privacidade, já que um dos principais desafios é o uso indevido das informações coletadas. Empresas e governos podem utilizar os dados obtidos por meio do reconhecimento facial para fins não autorizados, como monitoramento em massa, publicidade direcionada ou até mesmo discriminação com base em características físicas. O "reconhecimento facial tem se mostrado uma atualização *hightech* para o velho e conhecido racismo que está na base do sistema de justiça criminal e tem guiado o trabalho policial há décadas" (NUNES, p. 69-70, 2019).

A exposição dessas informações pode levar a violações da privacidade, prejudicando a liberdade individual e a dignidade humana.

A segurança dos dados pessoais é outra questão crítica. Os sistemas de reconhecimento facial dependem de bancos de dados que armazenam informações biométricas dos usuários. Esses dados são altamente sensíveis e, se não forem devidamente protegidos, podem ser alvo de ataques cibernéticos ou vazamentos, resultando em consequências graves, como roubo de identidade ou chantagem, perda da privacidade, do livre arbítrio e até mesmo da personalidade.

Por isso, é fundamental que sejam estabelecidas regulamentações e políticas adequadas para garantir a proteção dos dados pessoais em sistemas de reconhecimento facial. As legislações devem abordar aspectos como a obtenção do consentimento informado dos usuários, a finalidade específica da coleta de dados, a transparência na utilização e o direito de exclusão dos indivíduos. Além disso, é importante estabelecer padrões de segurança robustos para prevenir acessos não autorizados e garantir a criptografia adequada dos dados.

As empresas que desenvolvem e utilizam sistemas de reconhecimento facial também devem adotar uma postura ética e responsável. Isso implica em assegurar a conformidade com as normas de privacidade e segurança, bem como realizar auditorias e avaliações periódicas para garantir a conformidade contínua. Além disso, é essencial educar os usuários sobre os riscos e benefícios do uso dessa tecnologia, promovendo a conscientização e o engajamento.

A relação entre reconhecimento facial e proteção de dados pessoais é um desafio complexo que exige ações tanto no âmbito legislativo quanto no empresarial. A privacidade e segurança das informações biométricas devem ser salvaguardadas para garantir que os benefícios do reconhecimento facial sejam obtidos sem violar os direitos fundamentais dos indivíduos. Somente com uma abordagem equilibrada e responsável é possível garantir uma sociedade digital justa e preservar a privacidade na era da tecnologia.

Diante de uma ação na justiça impetrada pela Bancada Feminista através do mandato coletivo do PSOL - que demonstra a dinâmica das políticas públicas de poder ser influenciada pelo Poder Judiciário, mas essa influência só ocorre por causa da ação coletiva de organizações políticas e dos movimentos sociais - o TJSP (Tribunal de Justiça de São Paulo) suspendeu a compra de 20 mil câmeras de segurança com reconhecimento facial, que seriam adquiridas pela prefeitura da capital paulista, sob a preocupação de prática racista.[10]

> A decisão é do juiz de Direito Luis Manuel Fonseca Pires, da 3ª vara de Fazenda Pública. Magistrado apontou que essas câmeras com sistema de reconhecimento facial podem violar a LGPD - Lei Geral de Proteção de Dados e até apresentar "grave ameaça a direitos fundamentais", citando o risco de se reproduzir o racismo estrutural: A dimensão do impacto que o sistema tecnológico de monitoramento por reconhecimento facial produz impõe a responsabilidade ao Poder Público de apenas considerar o seu uso após a definição de regras legais precisas que ponderem os objetivos da segurança pública com os direitos fundamentais. Daí porque não há como adquirir o sistema de vídeo monitoramento sem se saber como esses dados podem ser processados (Lei Geral de Proteção de Dados) e como devem ser ponderados em proteção aos direitos fundamentais (CAVALCANTE; FERREIRA, 2023).

Neste mesmo sentido, pesquisa realizada por Pablo Nunes e divulgada pela *Intercept* Brasil resultou num levantamento alarmante onde revela que 90,5% dos presos por monitoramento facial no Brasil são negros. Rede de Observatórios de Segurança monitorou a tecnologia de reconhecimento facial em cinco estados. Resultado: além de ineficiente, sistema agrava o encarceramento de negros (NUNES, 2023).

Outra reportagem divulgada pelo *Intercept* Brasil, e escrita por Aiuri Rebello aponta que o delegado Waldir torrou R$ 30 milhões em reconhecimento facial para cidades que sequer têm saneamento em Goiás. (REBELLO , 2023)

Como afirma o filósofo e jurista Sílvio Almeida, “as instituições são apenas a materialização de uma estrutura social ou de um modo de socialização que tem o racismo como um dos seus componentes orgânicos. Dito de modo mais direto: as instituições são racistas porque a sociedade é racista” (ALMEIDA, 2017). O racismo estrutural incorporado e reproduzido em larga escala pela Administração Pública por meio do monitoramento de reconhecimento facial é uma realidade.

> O sistema de reconhecimento facial ainda ameaça gravemente o tratamento de dados pessoais, pois informações podem ser captadas, processadas e armazenadas em ampla escala sem qualquer consulta dos cidadãos cujas imagens são capturadas, e nesse particular há violação de relevantes fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei n. 13.709/2018 (PIRES, 2023).

Entretanto, a relação entre reconhecimento facial e discriminação surge principalmente no contexto da utilização dessa tecnologia por órgãos governamentais ou empresas. O risco está em como os dados coletados e processados podem ser utilizados para fins discriminatórios. Por exemplo, se os sistemas de reconhecimento facial forem treinados em conjuntos de dados que possuem vieses e desigualdades existentes, eles podem perpetuar essas discrepâncias e resultar em decisões discriminatórias, afrontando assim ao princípio da não discriminação estabelecido na LGPD.

Para evitar a relação problemática entre reconhecimento facial e discriminação, é fundamental que sejam tomadas medidas adequadas. Em primeiro lugar, é necessário garantir que os conjuntos de dados utilizados para treinar os algoritmos sejam representativos e imparciais, incorporando uma diversidade de grupos étnicos, raciais, de gênero e outras características relevantes. Além disso, é importante realizar testes regulares para identificar e corrigir vieses existentes nos sistemas.

Outra abordagem é a transparência e a prestação de contas. As empresas e os governos devem ser transparentes em relação ao uso de tecnologias de reconhecimento facial, divulgando informações sobre como os dados são coletados, armazenados, processados e utilizados. Isso permite que especialistas independentes avaliem a equidade e a segurança dos sistemas, garantindo a proteção dos direitos individuais.

Embora o reconhecimento facial e a discriminação sejam conceitos diferentes, é necessário estar atento às possíveis relações entre eles. A tecnologia de reconhecimento facial

pode apresentar riscos de discriminação se não forem tomadas precauções adequadas no desenvolvimento, treinamento e uso dos sistemas. É fundamental trabalhar em direção a soluções éticas, transparentes e imparciais para garantir que o reconhecimento facial seja uma ferramenta justa e equitativa, promovendo a igualdade e evitando a discriminação.

## 2.2 *Score* de crédito

O *score* de crédito é um sistema utilizado por instituições financeiras para medir o risco de crédito de um indivíduo. Com base em diversos fatores, como histórico de pagamentos, dívidas existentes, tempo de crédito e renda, o *score* de crédito atribui uma pontuação que reflete a probabilidade de uma pessoa cumprir com suas obrigações financeiras. Essa pontuação é frequentemente usada para determinar se um indivíduo é elegível para obter crédito e qual será o limite ou taxa de juros aplicados.

A discriminação, por outro lado, refere-se à prática injusta de tratar alguém de forma desigual com base em características como raça, gênero, idade, origem étnica, entre outros. A discriminação pode ocorrer em várias áreas da vida, incluindo o acesso a serviços financeiros. Quando se trata de crédito, a discriminação pode se manifestar de diferentes maneiras, como negar um empréstimo com base em características pessoais, aplicar taxas de juros mais altas em determinados grupos ou estabelecer requisitos mais rigorosos para certos indivíduos.

> A aferição e classificação do risco é *discrímen*. Deve se apoiar em critérios técnicos, mas, afinal, separa e valora para diversos efeitos, da avaliação do risco a sua precificação. Alguma discriminação na decisão de contratar ou na fixação do prêmio é necessária e inevitável (KEETON ; WIDISS ; FISCHER , 2017).
> O que se proíbe é que dos critérios resulte a discriminação injusta, considerada inaceitável, ou seja, os limites a esta atividade elementar da técnica securitária é do que desborde a critérios rejeitados pela ética social e jurídica contemporânea, consagrada no Direito, pela proteção dos direitos fundamentais (JUNQUEIRA, 2020).

Embora o *score* de crédito não seja uma forma explícita de discriminação, é importante considerar as implicações potenciais em termos de equidade e justiça. O sistema de pontuação é baseado em dados históricos e estatísticas que podem refletir disparidades sociais e econômicas existentes. Por exemplo, se determinados grupos demográficos historicamente enfrentaram dificuldades financeiras devido a desigualdades estruturais, isso pode resultar em pontuações de crédito mais baixas para esses grupos, o que pode limitar seu acesso a crédito e perpetuar as desigualdades.

Neste sentido, a discriminação proibida, contudo, não será apenas aquela baseada em características pessoais, “mas também as que se baseiem em fatos cuja adoção, uma vez

tomados como critério de diferenciação, tenham por consequência prejuízo ao seu titular, como pode ocorrer em relação ao exercício regular de um direito (art. 21 da Lei Geral de Proteção de Dados)" (JUNQUEIRA, 2020).

Além disso, o *score* de crédito pode estar sujeito a vieses algorítmicos. Os algoritmos usados para calcular o *score* de crédito são desenvolvidos com base em modelos estatísticos e de aprendizado de máquina. Se esses modelos forem treinados em conjuntos de dados que já possuem vieses e discriminação, isso pode se refletir nas decisões de crédito, resultando em tratamento desigual ou injusto para certos grupos.

Não é por outro motivo que um forte controle da informação é característica comum aos regimes totalitários. O Estado foi o primeiro a utilizar informações pessoais, por motivos razoavelmente claros:

> um pressuposto para uma administração pública eficiente é o conhecimento tão acurado quanto possível da população (não por acaso, à formação do *welfare state* seguiu-se um período de voraz demanda por informação pessoal por parte do Estado), o que implica, por exemplo, a realização de censos e pesquisas e o estabelecimento e regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública. Em relação ao controle, basta acenar às várias formas de controle social que podem ser desempenhadas pelo Estado e que seriam potencializadas com a maior disponibilidade de informações sobre os cidadãos, aumentando seu poder sobre os indivíduos (DONEDA, 2021).

Contudo, o controle da liberdade de subscrever do segurador encontra fundamentos, sobretudo, em aspectos existenciais – exemplificativamente, a tutela dos dados pessoais e a privacidade do candidato a segurado, o seu direito ao livre desenvolvimento da personalidade e a proteção dada pelo ordenamento jurídico contra a discriminação (art. 3º, inc. IV, da Constituição Federal).

Por isso, relacionar o *score* de crédito com a privacidade é uma abordagem interessante para entender os desafios e implicações éticas envolvidas na utilização de dados financeiros sensíveis para avaliar a elegibilidade e a confiabilidade dos indivíduos em relação ao crédito, pois conforme nos diz DONEDA, a falta de transparência nos critérios utilizados nos sistemas de classificação e avaliação, pode implicar

> ...entre outros atentados à dignidade da pessoa humana, possibilidades de discriminação social, etária, étnica e de gênero. Para minorar essa condição desfavorável ao cidadão, propõe-se à Autoridade Nacional de Proteção de Dados Pessoais a adoção de melhores práticas para maior controle, previsibilidade e explicabilidade nos processos automatizados que formam o *credit score* (DONEDA, 2021).

Nas sociedades de informação, como as nossas, pode-se dizer que ‘nós somos as nossas informações’, pois elas nos definem, nos classificam, nos etiquetam. A privacidade, hoje, manifesta-se, portanto, na capacidade de se controlar a circulação das informações. Saber quem as utiliza significa adquirir, concretamente, um poder sobre si mesmo. “Trata-se de uma concepção qualitativamente diferente da privacidade como ‘direito à autodeterminação informativa’, o qual concede a cada um de nós um real poder sobre as nossas próprias informações, os nossos próprios dados” (MORAES, 2010).

Neste sentido nos alerta Thiago Junqueira sobre o enfrentamento da discriminação algorítmica quando diz:

> Como se enfrentar a específica questão da discriminação algorítmica, porém, encontra-se em aberto. Para além da extraordinária multiplicação dos dados computáveis para fixação do prêmio, o que por si só gerará um desafio extra ao escrutínio da atuação do segurador, ainda que programados desconsiderando dados sensíveis, os algoritmos poderão causar discriminação (indireta e por “associação”) (JUNQUEIRA, 2020).

Para lidar com essas preocupações, as instituições financeiras e os provedores de *score* de crédito devem adotar práticas justas e transparentes. É necessário que eles realizem análises regulares para identificar e mitigar possíveis vieses nos modelos de pontuação, garantindo que não haja tratamento discriminatório. Além disso, é importante promover a diversidade e inclusão na indústria financeira, de forma que as perspectivas e experiências de diferentes grupos sejam consideradas na elaboração das políticas e práticas de crédito.

Embora o *score* de crédito e a discriminação sejam conceitos distintos, é válido compreender quais são as possíveis implicações éticas e desafios relacionados ao uso desses sistemas para avaliar a elegibilidade e o risco de crédito. É importante que o *score* de crédito seja desenvolvido e utilizado de forma justa, transparente e imparcial, levando em consideração as questões de equidade e evitando a perpetuação de discriminações e de desigualdades sociais e econômicas.

## 2.3 Processos seletivos de acesso a vagas de empregos

A automação tem se tornado uma parte cada vez mais presente em vários aspectos da vida moderna, incluindo o processo de seleção de emprego. Através de algoritmos e inteligência artificial, as empresas têm buscado automatizar partes desse processo, visando economia de tempo e recursos, além de uma suposta eficiência na identificação de candidatos qualificados.

No entanto, essa automação também pode trazer à tona questões preocupantes, como a discriminação.

No contexto do processo de seleção de emprego automatizado, a discriminação pode ocorrer de maneiras sutis, mas significativas. Os algoritmos utilizados para selecionar candidatos podem ser construídos com base em modelos de dados históricos que refletem desigualdades existentes na sociedade. Isso significa que se houver preconceito ou discriminação nos dados utilizados para treinar o algoritmo, ele pode aprender a reproduzir esses vieses durante o processo de seleção.

Por exemplo, se em um setor específico da indústria predominam candidatos de determinada etnia ou gênero, o algoritmo pode aprender a preferir automaticamente candidatos com características semelhantes. Isso resultaria em uma seleção que não leva em consideração as habilidades e qualificações individuais, mas sim estereótipos e preconceitos que perpetuam a exclusão de grupos minoritários.

Em 2018, a *Amazon* abandonou sua ferramenta própria de captação de talentos ao perceber que o sistema penalizava currículos que incluíam a palavra “mulheres”, como em “capitã do clube de xadrez de mulheres”, além de ter eliminado do processo pessoas formadas em duas instituições de ensino apenas para o sexo feminino.

Além disso, a automação do processo de seleção também pode levar à exclusão de candidatos com formações atípicas ou experiências não convencionais. Algoritmos podem ser programados para identificar palavras-chave específicas em currículos ou avaliar critérios arbitrários que podem não refletir a real capacidade de um candidato desempenhar uma função com sucesso. Isso pode excluir pessoas que, de outra forma, seriam altamente qualificadas, mas não se encaixam nos padrões rígidos definidos pelos algoritmos.

Para combater a discriminação no processo de seleção automatizado, é fundamental que as empresas estejam conscientes dos vieses e preconceitos potenciais presentes nos algoritmos que estão utilizando. É importante investir em treinamento e desenvolvimento de algoritmos éticos, levando em consideração a diversidade e inclusão como valores fundamentais. Além disso, é essencial realizar uma revisão humana dos resultados gerados pelos algoritmos, a fim de identificar possíveis casos de discriminação e corrigi-los.

A transparência também é um elemento chave nesse contexto. As empresas devem ser transparentes sobre o uso da automação no processo de seleção e comunicar claramente aos candidatos como as decisões são tomadas. Isso permite que os candidatos compreendam o processo e tenham a oportunidade de contestar possíveis discriminações.

Mesmo que a automação do processo de seleção de emprego ofereça benefícios em termos de eficiência, é fundamental estar atento aos riscos de discriminação que podem surgir. As empresas devem adotar uma abordagem ética e inclusiva na implementação de algoritmos, garantindo que a automação seja uma ferramenta que apoie a diversidade e a igualdade de oportunidades no ambiente de trabalho.

## 3. A ATUAÇÃO DO PODER JUDICIÁRIO PARA ATENDIMENTO AO PRINCÍPIO DA NÃO-DISCRIMINAÇÃO

A não discriminação é um princípio basilar para uma sociedade justa e igualitária. A LGPD reconhece a importância de assegurar que o tratamento de dados pessoais não resulte em qualquer forma de discriminação, seja ela de natureza racial, étnica, religiosa, política, genética, econômica ou de qualquer outra natureza. Isso é especialmente relevante no cenário atual, em que a tecnologia e a análise de dados têm um papel cada vez mais significativo na tomada de decisões que afetam a vida das pessoas em diversas esferas, como emprego, crédito, saúde e acesso a serviços.

Nesse contexto, a atuação do Poder Judiciário é essencial para garantir que os direitos dos cidadãos sejam respeitados. O Judiciário exerce o papel de guardião da Constituição e dos direitos fundamentais, e sua atuação é fundamental para coibir práticas discriminatórias no tratamento de dados pessoais. Casos de discriminação com base em dados pessoais devem ser levados ao Poder Judiciário para análise e decisão imparcial, de modo a proteger os indivíduos prejudicados e garantir que os responsáveis sejam responsabilizados de acordo com a legislação vigente.

Além disso, a atuação do Poder Judiciário contribui para o desenvolvimento de jurisprudência e interpretações sobre a aplicação do princípio da não discriminação na LGPD. À medida que os casos são julgados e as decisões são fundamentadas em princípios éticos e constitucionais, são criados parâmetros e orientações para a atuação dos demais atores envolvidos no tratamento de dados pessoais, como empresas, órgãos públicos e sociedade civil. Nesse sentido:

> Não há dúvidas de que os tribunais vêm exercendo um papel cada vez mais importante na política nacional e internacional em todo o mundo desde meados do século passado. Tanto em termos de quantidade quanto de impactos, seu envolvimento tem sido muito significativo. A decisão dos juízes vem ganhando peso sobre um amplo conjunto de questões, como no tratamento das minorias raciais, étnicas e sexuais; nos limites da liberdade religiosa e da reprodução humana; nos crimes contra os direitos humanos;

> no sentido dos direitos sociais; na punição da corrupção política; e na responsabilidade do Poder Executivo em matérias de segurança pública. (MCCANN, Michael W).

Dessa forma, o Poder Judiciário desempenha um papel indispensável na promoção e proteção da privacidade e dos direitos individuais previstos na LGPD. Sua atuação responsável e vigilante contribui para a construção de uma cultura de respeito à privacidade e não discriminação, incentivando a adoção de práticas transparentes, éticas e seguras no tratamento de dados pessoais.

## 3.1 Decisões Judiciais do Tribunal do Estado de São Paulo que mencionam o princípio da não discriminação

Diante da aplicabilidade do princípio da não discriminação e das implicações jurídicas e sociais que ele pode ter, foi escolhida uma metodologia de análise de ações judiciais no Tribunal de Justiça do Estado de São Paulo (TJSP) que tiveram como base a discussão sobre o atendimento a este princípio. Esta metodologia tem como objetivo compreender como o Judiciário tem interpretado e aplicado esse princípio em casos concretos, contribuindo para uma reflexão mais aprofundada sobre o tema.

Inicialmente, foram selecionadas ações judiciais que apresentavam como ponto central a discussão sobre a proteção de dados pessoais e a não discriminação, incluindo casos envolvendo empresas, instituições públicas e outros atores que tratam dados de cidadãos. Em seguida, foram analisados os argumentos apresentados pelas partes envolvidas, bem como os fundamentos utilizados pelos magistrados para chegarem as suas decisões.

Durante a análise, se pretendeu identificar as nuances e desafios enfrentados pelas partes para demonstrar se houve ou não violação do princípio da não discriminação previsto na LGPD. Além disso, foram observadas as circunstâncias específicas de cada caso para assim verificar se elas podem ter influenciado a interpretação da lei e as decisões dos tribunais.

Essa abordagem metodológica possibilitou uma visão abrangente e aprofundada do tema, contribuindo para a compreensão das principais questões relacionadas ao princípio da não discriminação na LGPD e sua efetiva aplicação no cenário jurídico paulista.

Os resultados obtidos com a análise das ações judiciais do TJSP revelam a complexidade do tema da não discriminação na proteção de dados pois se observa que, em muitos casos, os magistrados têm buscado aplicar o princípio de forma rigorosa para evitar abusos no tratamento de dados e garantir a igualdade e dignidade dos indivíduos envolvidos.

Entretanto, ficou evidenciada a existência de desafios na aplicação prática da LGPD e na interpretação do princípio da não discriminação. A lei é recente, e a tecnologia e os modelos de negócio evoluem rapidamente, o que pode gerar dificuldades para acompanhar as mudanças e garantir o pleno cumprimento da legislação.

Dessa forma, a análise das ações judiciais do TJSP relacionadas ao princípio da não discriminação na LGPD, proporcionou um panorama mais amplo e crítico sobre a efetividade da legislação e a aplicação das normas de proteção de dados no contexto jurídico brasileiro, já que o amadurecimento da LGPD no Brasil tem sido uma evolução significativa para a proteção da privacidade e dos dados pessoais dos cidadãos, porém se constata que a maioria das ações judiciais impetradas estão concentradas no Estado de São Paulo.

> As decisões permanecem concentradas no Tribunal de Justiça do Estado de São Paulo (TJSP), onde foram apreciadas 110 ações entre setembro de 2021 e setembro de 2022, ante 68 identificadas no levantamento anterior. Após a Corte paulista, o TJBA (11), o TJRS (10) e o TJDFT (9) são os que têm o maior número de decisões sobre LGPD.

Desta maneira, a opção pela pesquisa direcionada ao TJSP se justifica pelo fato de que das 629 ações que debatem sobre a LGPD 570 foram iniciadas em SP. Das 570 ações foram apreciadas 110 ações, e dentre elas 21 destacam o princípio da não discriminação como base para o voto proferido. Dentre as 21 ações, participaram do julgamento dos recursos os desembargadores Anna Paula Dias Da Costa, Spencer Almeida Ferreira e Fernando Sastre Redondo. Sendo que em 16 destas ações a desembargadora Anna Paula Dias da Costa, utilizou como fundamento o artigo 6º, IX (não discriminação), nos quais atuando como relatora teve o seu voto acompanhado pela maioria, para dar provimento aos recursos que favoreciam consumidores que tiveram o nome indevidamente negativado junto ao SERASA, uma vez que considerou as discriminações sofridas como abusivas.

Por fim, nos próximos tópicos analisarei duas ações judiciais, uma relacionada à utilização de biometria no metrô de São Paulo e a outra ação utilizo um dos votos proferidos pela desembargadora acima apontada cuja argumentação e embasamento são utilizados nas outras quinze ações que questionaram a ilicitude e a abusividade de discriminações que foram utilizadas no tratamento de dados pessoais e que ganharam destaque na aplicabilidade da LGPD.

### 3.1.1 Ajuizamento de Ação Civil Pública contra o Uso de Reconhecimento Facial pela Companhia do Metropolitano de São Paulo - Processo nº 1090663-42.2018.8.26.0100 – 8ª Câmara de Direito Público. TJSP. Agravo de Instrumento. Acórdão.

O reconhecimento facial é uma dessas tecnologias que requer cuidados e regulamentação adequada. No caso específico da Companhia do Metropolitano de São Paulo (Metrô), o ajuizamento de uma Ação Civil Pública se fez necessário para assegurar que não haja qualquer captação de dados biométricos de forma abusiva e ilícita, evitando, assim, possíveis formas de discriminação no uso do transporte público.

O reconhecimento facial é um sistema que utiliza algoritmos para identificar e verificar indivíduos com base em suas características faciais, e embora seja uma ferramenta promissora em áreas como segurança e prevenção de crimes, seu uso indiscriminado em ambientes públicos pode ameaçar a privacidade dos cidadãos e potencialmente levar a práticas discriminatórias. Isso porque, em sua essência, o reconhecimento facial pode levantar questões sobre vigilância em massa e o tratamento desigual de determinados grupos sociais.

No contexto do transporte público, o uso do reconhecimento facial pela Companhia do Metrô de São Paulo para identificar passageiros poderia suscitar preocupações válidas. Primeiramente, existe o risco de que dados sensíveis dos usuários sejam coletados e armazenados sem o devido consentimento, o que pode violar o direito fundamental à privacidade e à proteção de dados pessoais. Além disso, considerando a diversidade da população e as possíveis limitações técnicas dos sistemas de reconhecimento facial, pode haver erros de identificação, levando a falsas acusações ou constrangimentos para indivíduos inocentes.

Quando o reconhecimento facial é empregado de forma obscura, sem que saibamos como nossas informações são utilizadas e compartilhadas, corre-se o risco de se tolher não só a liberdade como a democracia.

A falta de transparência no uso do reconhecimento facial como consequência levanta preocupações quanto à discriminação e injustiça. Se os algoritmos utilizados não forem devidamente regulados e fiscalizados, há o risco de viéses incorporados nos sistemas, resultando em decisões injustas que afetam desproporcionalmente certos grupos da sociedade. Essa falta de equidade mina os princípios democráticos de igualdade e justiça, já que alguns cidadãos podem ser alvo de monitoramento excessivo, enquanto outros passam despercebidos. Por isso, é crucial que qualquer uso de reconhecimento facial seja acompanhado por

regulamentações rigorosas, transparência completa e salvaguardas para garantir que os direitos individuais sejam respeitados e que a igualdade perante a lei seja mantida intacta, pois conforme nos alerta Carissa Véliz:

> Cada imagem, palavra e clique é coletado, monetizado por empresas, examinado e potencialmente dilacerado em um ato público catártico de humilhação virtual por parte dos internautas. Essa confusão constante em razão de cada detalhe do que as pessoas dizem e fazem nos distrai de conversas mais importantes – de falar sobre questões de justiça, economia, ecologia e bens públicos (VELIZ, p.156, 2021)

A discriminação no uso do transporte público é uma preocupação legítima e deve ser tratada com seriedade. O reconhecimento facial pode ser suscetível a vieses, pois os algoritmos são treinados com base em conjuntos de dados que podem refletir preconceitos e desigualdades presentes na sociedade. Isso pode levar a uma maior vigilância ou tratamento desigual de determinados grupos, como minorias étnicas, pessoas de baixa renda ou indivíduos com deficiências. Portanto, é fundamental que medidas preventivas sejam adotadas para garantir que o transporte público seja um espaço inclusivo e acessível a todos.

Consta na petição inicial da referida ação civil que em 12 de abril de 2018, que

> A concessionária Via Quatro que opera a Linha 4-Amarela de metrôs na cidade de São Paulo e figura como parte ré da presente ação, anunciou a instalação, no dia 18 do mesmo mês, de "portas de plataforma interativas nas estações Luz, Paulista e Pinheiros, com funcionamento durante todo o horário de operação da linha". Segundo a empresa, a tecnologia implementada nessas portas consiste em uma lente com um sensor que "reconhece a presença humana e identifica a quantidade de pessoas que passam e olham para tela". O foco da ferramenta é também a identificação de emoção (raiva, alegria, neutralidade), gênero e faixa etária das pessoas posicionadas em frente ao sensor.

Em sua defesa, alegou o metrô que:

> A tecnologia embarcada nas Portas Interativas Digitais se limita a contar as pessoas, visualizações, tempo de permanência, tempo de atenção, gênero, faixas etárias, emoções, fator de visão, horas de pico de visualizações e distância de detecção, sem que para isso colete qualquer dado pessoal de pessoa individualizada. Apenas são gerados dados meramente estatísticos.

Na sentença de fls. 2298 e 2299 a juíza acolheu quase que integralmente o pedido dos requerentes afastando somente a condenação em danos morais e proferiu:

> Ante o exposto, JULGO PROCEDENTES EM PARTE os pedidos, com resolução do mérito, na forma do artigo 487, I do Código de Processo Civil, para (i) determinar que a requerida se abstenha de captar as imagens, sons e quaisquer outros dados pessoais

> dos consumidores usuários, através das câmeras ou outros dispositivos envolvendo os equipamentos instalados na Linha 4, Amarela do metrô, sem consentimento prévio do consumidor, confirmando a liminar anteriormente concedida pela decisão de fls. 327/332; (ii) determinar à requerida que, caso deseje readotar as práticas tratadas nos autos, deverá obter o consentimento prévio dos usuários mediante informação clara e específica sobre a captação e tratamento dos dados, com adoção das ferramentas pertinentes; e (iii) condenar a requerida ao pagamento de indenização por danos morais coletivos no valor de R$100.000,00, corrigida segundo a tabela prática do Egrégio Tribunal de Justiça de São Paulo desde a data da publicação da sentença, e com juros demora de 1% ao mês, incidentes a partir da citação, por se tratar de ilícito contratual, na forma do artigo 405, do Código Civil, a ser revertido para o Fundo de Defesa de Direitos Difusos FDD, criado na forma do artigo 13 da Lei nº 7.347/85[11].

Na sentença proferida, a juíza também esclareceu que o metrô não comprovou que as imagens captadas eram utilizadas meramente para fins estatísticos, bem como, que:

> Ainda que se constatasse concretamente a ausência de efetivo reconhecimento facial pelo equipamento instalado, não há dúvidas de que há captação da imagem de usuários, sem o seu conhecimento ou consentimento para fins comerciais que beneficiam a ré e a empresa por ela contratada[12].

Da sentença acima houve interposição de recurso ao Tribunal de Justiça de São Paulo e o relator da apelação, desembargador Antônio Celso Faria, classificou a conduta da empresa como reprovável e ofensiva à moral coletiva, ressaltando que

> É praticamente impossível calcular o número de passageiros que utilizam a plataforma da ré diariamente, fato que caracteriza o dano moral coletivo.
> Os cidadãos transportados pela concessionária Via Quatro, estão sendo invadidos na sua intimidade, com fins lucrativos, ou mesmo outros fins obscuros, sem que isso seja autorizado e sem que haja um controle mínimo sobre a utilização de captação de imagens, bem como não se tenha a menor ideia de quanto isso representa ou representará de lucro para a concessionária.
> (...)
> Restou incontroverso de que a captação das imagens, ora discutidas, eram utilizadas para fins publicitários e comerciais, tendo-se em vista que se buscava detectar as principais características dos indivíduos que circulavam em determinados locais e horários, bem como emoções e reações apresentadas à publicidade veiculada no equipamento. Ademais, é fato incontroverso que os usuários não foram advertidos ou comunicados prévia ou posteriormente acerca da utilização ou captação de sua imagem, o que afronta, claramente, o direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais.
> (...)
> À ré, na condição de concessionária de serviço público, incumbe arcar com o risco das atividades econômicas que explora, especialmente por envolver os direitos fundamentais à intimidade, à privacidade, à imagem e à honra dos usuários consumidores, o que não ocorreu.

---

[11] Site https://esaj.tjsp.jus.br/pastadigital/sg/abrirConferenciaDocumento.do, informe o processo 1090663-42.2018.8.26.0100 e código 2059FA43, acesso em 22 de maio de 2023.
[12] Site https://www.migalhas.com.br/quentes/386303/tj-sp-via-quatro-e-condenada-em-r-500-mil-por-coleta-de-dados acesso em 06 de junho de 2023

Por fim, a 8ª Câmara de Direito Público do TJ/SP manteve a condenação da Via Quatro, concessionária da Linha Amarela do Metrô de São Paulo, por utilizar indevidamente o sistema de câmeras de segurança para captação de imagens de usuários com fins comerciais e publicitários. O órgão colegiado votou pelo aumento do valor sentenciado do dano moral coletivo, que foi fixado em R$ 500 mil e será revertido para o Fundo de Defesa de Direitos Difusos (FDD).

O ajuizamento de Ação Civil Pública para que a Companhia do Metrô de São Paulo se abstenha do uso de qualquer mecanismo ou sistema de captação de dados biométricos para reconhecimento facial serve como um alerta da Defensoria Pública da União, IDEC - Instituto Brasileiro de Defesa do Consumidor, INTERVOZES - Coletivo Brasil de Comunicação Social, e Artigo 19 Brasil de que o sistema de reconhecimento facial implementado pelo metrô de SP não atende aos requisitos previstos não só no Código de Defesa do Consumidor, no Código de Usuários de Serviços Públicos, no Estatuto da Criança e do Adolescente, na Constituição Federal e nos tratados internacionais como na LGPD:

> A Lei Geral de Proteção de Dados estabelece que tratamento de dados pessoais, inclusive nos meios digitais, deve ter como fundamento o respeito aos direitos humanos, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º), sendo que a atividade de tratamento de dados pessoais deve observar o princípio da não discriminação (art. 6 º), do que decorre a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos[13].

Essa ação teve como objetivo garantir que os direitos fundamentais dos passageiros fossem respeitados, protegendo a privacidade e evitando a discriminação injusta. Além disso, é uma oportunidade de abrir um importante debate sobre o uso ético e responsável de tecnologias de reconhecimento facial em espaços públicos.

> Parte central da ação aponta que as tecnologias de reconhecimento facial elevam exponencialmente o risco de discriminação de pessoas negras, não binárias e trans já que esse tipo de tecnologia é reconhecidamente falho em sua acurácia e imerso em ambiente de racismo estrutural. O documento sustenta que mesmo os melhores algoritmos dispõem de pouca precisão ao realizar o reconhecimento de pessoas negras e transgênero, que são mais afetadas por falsos positivos e falsos negativos e ficam mais expostas a constrangimentos e violações de direitos. A ação também questiona o uso de imagem e a coleta e tratamento de dados pessoais sensíveis de crianças e adolescentes, sem que haja o consentimento dos pais ou responsáveis, em frontal violação ao que determina a LGPD, o ECA e a proteção constitucional[14].

[13] Site https://www.migalhas.com.br/quentes/360681/acao-questiona-uso-de-reconhecimento-facial-no-metro-de-sp, acesso em 23 de maio de 2023.
[14] Idem

Portanto, cabe às autoridades competentes, à sociedade civil e às empresas, como a Companhia do Metrô de São Paulo, trabalhar juntos para encontrar soluções que permitam o uso da tecnologia de forma responsável, respeitando os direitos e a dignidade de todos os cidadãos.

Segundo Zygmunt Bauman, existe um abismo sobre o que deveria ser o indivíduo na sociedade e o que ele é de fato uma vez que não é ele quem controla o seu próprio destino e por isso compete a Política com P maiúsculo, oferecer meios para que consigamos ter o controle do nosso destino:

> Há um grande e crescente abismo entre a condição de indivíduos *de jure* e suas chances de se tornar indivíduos *de facto* -isto é, de ganhar controle sobre seus destinos e tomar as decisões que em verdade desejam. É esse abismo, que emanam os eflúvios mais venenosos que contaminam as vidas dos indivíduos contemporâneos. Esse abismo não pode ser transposto apenas por esforços individuais: não pelos meios e recursos disponíveis dentro da política-vida autoadministrada. Transpor o abismo é a tarefa da Política com P maiúsculo. Pode-se supor que o abismo em questão emergiu e cresceu precisamente por causa do esvaziamento do espaço público, e particularmente da ágora, aquele lugar intermediário, público/privado, onde a política-vida encontra a Política com P maiúsculo onde os problemas privados são traduzidos para a linguagem das questões públicas e soluções públicas para os problemas privados são buscadas, negociadas e acordadas (BAUMAN, p. 53, 2021).

Assim, se verifica que no caso desta ação civil pública a crescente conscientização sobre a importância da privacidade e proteção de dados tem impulsionado a atuação de organizações e movimentos da sociedade civil na mobilização do direito para assegurar o cumprimento efetivo da Lei Geral de Proteção de Dados (LGPD).

A atuação proativa da sociedade civil desempenha um papel de pressão e cobrança junto ao Poder Público para garantir que a LGPD não seja apenas uma lei no papel, mas uma realidade efetivamente aplicada. Organizações têm desempenhado um papel crucial ao monitorar as ações de empresas e instituições públicas, denunciando violações e descumprimentos da lei, e buscando a responsabilização dos infratores. Através de ações judiciais, petições públicas e mobilização sociais, esses grupos têm exercido uma influência significativa na agenda pública, forçando as autoridades a tomar medidas concretas para garantir a implementação adequada da LGPD.

### 3.1.2 Processo nº 1001822-16.2021.8.26.0246 da 2ª Vara do Foro de Ilha Solteira/SP. Práticas Abusivas. 38ª Câmara de Direito Privado. TJSP. Apelação. Acórdão.

Os cadastros negativos contêm dados sobre as dívidas não pagas dos consumidores e são mantidos em bancos de dados de pessoas jurídicas de direito privado que prestam esses serviços para os fornecedores nas relações de consumo, como o Serviço de Proteção ao Crédito (SPC Brasil), o Serviço Central de Proteção ao Crédito (SCPC) e a Serasa Experian. Enquanto os dois primeiros têm bancos de dados formados principalmente por comerciantes e outros prestadores de serviços, a terceira é voltada especialmente para as instituições financeiras.

Antes da LGPD, as empresas de cadastros negativos utilizavam os dados pessoais de qualquer pessoa viva sem que o seu titular soubesse onde, como e por quê o mesmo estava sendo utilizado, e por este fato as empresas privadas ou até mesmo públicas utilizavam-se desses dados com diversos objetivos que ultrapassavam a área do econômico, e ganhavam proporções até mesmo inimagináveis.

Contudo, após a entrada em vigor da LGPD, o que vemos é que órgãos como o SERASA estão sendo cada vez mais questionados com relação a forma com que utilizam o gigantesco banco de dados pessoais que possuem em seu poder e por isto, agora se torna cada vez mais comum notícias de que medidas judiciais estão sendo tomadas para que seja atendida a referida lei, como estas aqui:

> O juiz substituto da 5ª Vara Cível de Brasília confirmou decisão liminar da 2ª Turma Cível do TJDFT que determinou que a Serasa Experian pare de comercializar dados pessoais dos titulares por meio dos produtos Lista Online e Prospecção de Clientes, oferecidos pelo site da ré, sob pena de imposição das medidas para assegurar o cumprimento da ordem judicial, conforme legislação vigente.
> A Ação Civil Pública foi proposta pelo MPDFT, sob o argumento de que a venda dos dados fere a Lei Geral de Proteção de Dados Pessoais – LGPD, uma vez que a norma impõe a necessidade de manifestação específica para cada uma das finalidades de tratamento dos dados. Logo, o compartilhamento de tais informações, da forma que tem sido feita pela empresa, seria ilegal ao ferir o direito à privacidade das pessoas, bem como os direitos à intimidade, privacidade e honra dos titulares dos dados[15].

Neste caso, a Ação Civil Pública foi proposta pelo Ministério Público, do Distrito Federal, que tem entre as suas funções garantir a proteção do direito coletivo à proteção dos dados pessoais, uma vez que foi verificado que qualquer empresa que contrate o serviço do SERASA tem acesso a informações de mais de 150 milhões de CPFs, o que pode gerar um grande vazamento de dados pessoais.

---

[15] LGPD: Justiça confirma liminar e determina que Serasa deixe de comercializar dados pessoais. Site: https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/julho/lgpd-justica-determina-que-serasa-deixe-de-comercializar-dados-pessoais. Acesso em 30 de julho de 2023.

A decisão citada acima, vai de encontro com o pensamento da filósofa Véliz, que nos diz que há quatro maneiras principais de se envenenar as sociedades com a má administração de dados pessoais. Os dados pessoais podem comprometer a segurança nacional, podem ser usados para corromper a democracia, podem ameaçar as sociedades liberais ao promover uma cultura de exposição e vigilantismo, e podem colocar em risco a segurança dos indivíduos (p. 137, 2021).

Desta maneira, se percebe uma mudança provocada pela LGPD que faz com que haja um aumento significativo de ações judiciais que questionam a utilização sem amparo legal de dados pessoais por empresas que contratam os serviços de órgãos de proteção ao crédito sem que haja qualquer hipótese de autorização legal ou do titular para o seu tratamento.

Neste sentido, para verificarmos a tendência cada vez maior dos Tribunais, principalmente do Tribunal de Justiça de São Paulo, de amparar as decisões judiciais no princípio da não discriminação para freiar a negativação dos consumidores frente aos órgãos de proteção ao crédito, cabe a análise também da ação que consta no título deste tópico cuja ementa segue abaixo:

> INDENIZAÇÃO.
> Serasa "Limpa Nome". Incidência do CDC. Divulgação de informações de dados do consumidor amparada em dívida prescrita. Abusividade. Comprovado o acesso de terceiros às informações registradas nos cadastros de serviços de proteção ao crédito. Inteligência do art. 43, § 5º, do CDC. Inscrição que influencia de forma negativa a pontuação do score do consumidor. Plataforma de proteção do crédito que visa alertar os fornecedores sobre eventuais maus pagadores. Prática que viola os artigos 6º, IX e 7º, X, da Lei nº 13.853/2019 – Lei Geral de Proteção de Dados Pessoais (LGDP). Infringência ao disposto no art. 882 do Código Civil. Dano moral configurado. Quantum fixado em observância aos critérios de razoabilidade e proporcionalidade. Calibrada a verba honorária de sucumbência. Precedentes desta C. Câmara. Sentença reformada. RECURSO PROVIDO[16].

Na inicial, a parte autora do caso em questão alegou estar sendo persistentemente cobrada pela empresa demandada. Diante dessa situação, após realizar uma consulta aos órgãos de restrição de crédito, especificamente no site da Serasa, constatou que as cobranças se relacionavam a uma dívida originada junto ao Banco Losango. No entanto, ela sustenta que a referida dívida está prescrita, o que significa que não é mais exigível legalmente. Para embasar sua argumentação, a autora anexou um documento contendo detalhes de uma proposta de acordo.

[16]Site:https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=6U0001EFH0000&processo.foro=246&processo.numero=1001822-16.2021.8.26.0246 . Acesso em 17 de junho de 2023.

Conforme preconizado pelo artigo 71 do Código de Defesa do Consumidor (CDC), à ausência de legitimidade para realizar a cobrança, baseando-se no artigo 206, § 5º, I, do Código Civil, e à manutenção de informações prejudiciais ao acesso futuro ao crédito por um período superior a 5 anos no cadastro de inadimplentes, contrariando os dispositivos § 1º e 5º do artigo 43 do CDC, a autora optou por ajuizar a ação judicial.

O Banco requerido, em sua defesa argumentou, de forma resumida, que a autora adquiriu a dívida por meio de cessão de crédito, o que, lhe confere legitimidade para conduzir a cobrança de maneira extrajudicial. Além disso, alegou que o nome da autora não estava negativado, mesmo que aparecesse em um portal de negociação conhecido como Serasa Limpa Nome. O Banco destacou que apenas os consumidores com cadastro na plataforma poderiam acessar essas informações. Portanto, alegou a ausência de fundamento para alegações de dano moral passível de indenização.

No desenrolar do processo, a ação foi objeto de julgamento parcialmente procedente onde foi declarada a inexigibilidade da dívida devido à prescrição, o que significa que a dívida não poderia mais ser legalmente cobrada devido ao transcurso do tempo desde sua origem e o pedido de condenação por danos morais foi rejeitado pelo tribunal.

Interposto contra a sentença, recurso de apelação e contrarrazões, a menção ao princípio da não discriminação se faz quando a desembargadora relatora designada Anna Paula Dias da Costa apontou para a abusividade na indução ao consumidor na contratação de uma nova dívida para quitar a anterior, e como fundamentação a desembargadora utilizou o artigo 6º, IX (não discriminação) e o artigo 7º, X, da LGPD para dizer:

> Trata-se de uma forma abusiva (maquiada com benevolências turbinar o *score*) de induzir o consumidor a pagar dívida prescrita e contrair agora uma nova dívida, que se inadimplida pode gerar restrição em seu nome. Esta prática, inclusive, viola o disposto no artigo 6º, IX, da Lei nº13.853/2019 Lei Geral de Proteção de Dados Pessoais (LGDP), in *verbis:*
> Art. 6º "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> (...) IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
> Sucede que, a partir da LGPD o tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as empresas devem explicar para que irão usar cada um dos dados pessoais, uma vez que não é possível tratá-los com finalidades genéricas ou indeterminadas. Neste contexto, os dados dos consumidores que constam no campo "contas atrasadas", estão em desacordo com a norma prescrita do artigo 7º, X, do referido diploma legal. Confira-se:
> Art. 7º "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

> (...)X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. [17]

Este caso exemplifica um embate jurídico complexo, no qual questões de cobrança indevida, prescrição de dívida e interpretações das leis de proteção ao consumidor se entrelaçam. As nuances legais e as provas apresentadas pelos envolvidos foram determinantes para o desfecho da ação, evidenciando a importância do sistema judiciário no equilíbrio das relações comerciais e na garantia dos direitos dos consumidores.

A cobrança abusiva, ainda que de débito existente, é vedada desde o ano de 1990 pelo Código de Defesa do Consumidor, conforme se verifica em seu artigo 42 que estabelece:

> Art. 42. Na cobrança de débitos, o consumidor inadimplente não será exposto a ridículo, nem será submetido a qualquer tipo de constrangimento ou ameaça.
> Parágrafo único. O consumidor cobrado em quantia indevida tem direito à repetição do indébito, por valor igual ao dobro do que pagou em excesso, acrescido de correção monetária e juros legais, salvo hipótese de engano justificável.

Contudo, a desembargadora ao trazer em sua fundamentação os artigos 6º e 7º da LGPD ela reconhece que a proteção e a privacidade de dados pessoais ultrapassa o constrangimento ou ameaça sentida pelo consumidor e alcança o reconhecimento da discriminação neste caso considerada abusiva, recebendo assim amparo também constitucional que recentemente estabeleceu que este direito não só é abrangido pela área consumerista, ou de dados pessoais mas sim é também um direito fundamental.

Desta maneira, considerando que a negativação do nome da consumidora junto ao SERASA, de forma abusiva poderia lhe trazer prejuízos que ultrapassam o âmbito econômico uma vez que os seus dados pessoais estavam disponíveis para acesso de empresas privadas e públicas se verifica que:

> Nossas vidas, traduzidas em dados, são a matéria-prima da economia de vigilância. Nossas esperanças, nossos medos, o que lemos, o que escrevemos, nossas relações, nossas doenças, nossos erros, nossas compras, nossas fraquezas, nossos rostos, nossas vozes – tudo é usado como alimento para abutres de dados que coletam tudo, analisam tudo e vendem tudo a quem der o maior lance. Muitos daqueles que adquirem nossos dados os querem para fins nefastos: para trair nossos segredos em benefício de companhias de seguros, empregadores e governos; para nos vender coisas que não temos interesse em comprar; para nos colocar uns contra os outros em um esforço de implodir nossa sociedade; para nos desinformar e tomar o controle de nossas democracias. A sociedade de vigilância transformou *os cidadãos* em *usuários* e *titulares* de dados (VÉLIZ, p.23, 2021).

[17]Site:https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=6U0001EFH0000&processo.foro=246&processo.numero=1001822-16.2021.8.26.0246 . Acesso em 17 de junho de 2023.

Inserir a proteção de dados no rol de direitos fundamentais, demonstra a necessidade de se proteger direitos atinentes a situações jurídicas sem as quais a pessoa não consegue se desenvolver, não se realiza, não convive e, às vezes, nem mesmo sobrevive.

Assim, o reconhecimento da proteção de dados pessoais como direito fundamental, legitima um dos objetivos da LGPD como previsto também em seu artigo 1º, que nos assegura o livre desenvolvimento da personalidade, a liberdade e a privacidade, e assim também alcança os direitos previstos no Código de Defesa do Consumidor, principalmente quando acompanhamos os efeitos resultantes das discriminações negativas presentes em nossas vidas, pois a ausência, ou a mera falta de clareza, das normas – anomia – é o pior que pode acontecer às pessoas em sua luta para dar conta dos afazeres da vida ( BAUMAN, p.30, 2021).

Se percebe que a conscientização dos direitos dos titulares de dados pessoais faz com que cada vez mais sejam iniciadas ações em âmbito judicial que questionam a prescrição de dívidas que agora também encontra amparo nesta política regulatória representada pela LGPD. Mesmo porque como a desembargadora menciona na referida ação, que as informações disponibilizadas no SERASA estão disponibilizadas a terceiros e podem influenciar a pontuação do score da consumidora e como a dívida estava prescrita a juíza argumentou que se trataria de forma abusiva de induzir a consumidora a pagá-la violando assim a LGPD.

Desta forma se constata que as decisões judiciais, principalmente aquelas preferidas pela desembargadora do TJSP, tendem a considerar que a discriminação abusiva e ilícita no colhimento de dados pessoais não será apenas aquela baseada em características pessoais, mas também as que se baseiam em fatos cuja adoção, uma vez tomados como critério de diferenciação, tenham por consequência prejuízo ao seu titular, como pode ocorrer em relação ao exercício regular de um direito (JUNQUEIRA, p. 13, 2020).

Em um contexto de avanços tecnológicos e constantes mudanças no cenário de colhimento de dados pessoais, a observação cuidadosa das decisões judiciais relacionadas à LGPD torna-se fundamental para garantir a efetividade e a aplicação coerente desta legislação. A análise constante das resoluções judiciais não apenas assegura que o princípio da não discriminação da LGPD seja atendido, mas também auxilia na adaptação e interpretação da lei diante de situações complexas e novos desafios que emergem nesse ambiente em constante transformação. Ao monitorar e avaliar como os tribunais lidam com casos envolvendo proteção

de dados, é possível promover um ambiente legal sólido e consistente, garantindo a salvaguarda dos direitos individuais e a construção de uma cultura de privacidade sólida.

## 4. MOBILIZAÇÃO POLÍTICA E DIREITO: IMPLEMENTAÇÃO DE UMA POLÍTICA PÚBLICA REGULATÓRIA COMO FORMA DE ADAPTAÇÃO A NOVA REALIDADE DE COLHIMENTO DOS DADOS PESSOAIS

### 4.1 Conceito de política pública regulatória

A política pública regulatória é um conceito essencial no âmbito da administração pública e governança, pois visa estabelecer regras, normas e diretrizes para orientar o funcionamento de setores específicos da sociedade. Em sua essência, trata-se da criação de normativas e instrumentos governamentais com o objetivo de regular e controlar a atuação de empresas, organizações e indivíduos em determinadas áreas, a fim de promover o bem-estar social, a justiça e o equilíbrio entre os diversos interesses envolvidos. Nesse sentido Muzzi, traz a tipologia de Lowi para demonstrar o alcance das políticas públicas na sociedade:

> A tipologia de Lowi, autor responsável por uma revolução na relação causal entre o exercício político e a política pública, fundamenta-se no impacto que a política pública pretende ter na sociedade, criando, portanto, quatro tipos: políticas regulatórias, que determinam os padrões de comportamento da sociedade; políticas distributivas, que direcionam recursos difusos da coletividade para grupos específicos de interesses; políticas redistributivas, que concedem benefícios a um grupo específico, retirando recursos de outros grupos também específicos de atores; e as políticas constitutivas, que definem as regras que irão moldar o funcionamento da sociedade e do governo" (MUZZI ,p.16, 2014).

O Estado exerce funções com o objetivo de atender demandas e de promover mudanças significativas por intermédio de decisões. "As ações necessárias para alcançar tais objetivos são tomadas através das chamadas políticas públicas, um conjunto de ações e decisões do governo, voltadas para a solução (ou não) de problemas da sociedade" (LOPES; AMARAL, 2008).

A presente pesquisa teve por base a análise de um princípio previsto na LGPD que é considerada como política pública constitutiva, ou seja, regulatória, que, de acordo com Schmidt (2018), "é a que regula e estabelece ordens, proibições, decretos, portarias afetando diretamente o comportamento dos cidadãos". Desta maneira, e como nos diz Subirast (2008) "devemos observar a política pública não como um esquema rígido, mas sim como um marco referencial, imaginando-a como um fluxo contínuo de decisões e procedimentos".

Uma política pública regulatória tem como premissa básica a necessidade de intervenção estatal em atividades que impactam a coletividade, mas que, se não regulamentadas, poderiam gerar externalidades negativas ou desequilíbrios no mercado. O Estado assume o papel de regulador para garantir o interesse público, proteger os direitos dos cidadãos e garantir o desenvolvimento sustentável. Desta forma,

> A Análise de Política, por sua vez, coloca em pauta tanto a política quanto a política pública, visto que, por um lado, procura conhecer as ações do governo, descrevendo-as, e, por outro, analisa e prescreve as políticas públicas. (ESTEVÃO; FERREIRA, p.169, 2018)

As áreas mais comuns em que as políticas públicas regulatórias são aplicadas incluem: meio ambiente, saúde, educação, transporte, telecomunicações, energia, finanças, entre outras. Cada uma dessas áreas possui suas peculiaridades, necessidades e desafios específicos, o que demanda a formulação de políticas adequadas e personalizadas.

A formulação de uma política pública regulatória passa por diversas etapas. Primeiro, é realizada uma análise detalhada do setor em questão, levando em conta suas características, atores envolvidos, impactos socioeconômicos e objetivos a serem alcançados. Em seguida, são estabelecidos os princípios e diretrizes que nortearão a regulamentação, sempre buscando o equilíbrio entre os interesses dos diferentes grupos afetados.

Frey (2000) observa que “o ciclo de políticas públicas acaba sendo bastante interessante para a análise de uma política pública já que as várias fases correspondem a uma sequência de elementos do processo político-administrativo que podem ser investigados no que diz respeito a alguns aspectos basilares dela”. Contudo, há aqui uma visão bastante “neutra”, “idealizada”, do que, de fato, representa uma política pública. A transformação de determinada questão em um “problema público” e, posteriormente, em “problema político” (quando, de fato, entra na agenda governamental) é uma perspectiva de análise mais pertinente para o caso em questão. Isso porque, pensar o ciclo da política em si, não diz muito sobre o seu conteúdo.

Por isso, um aspecto importante das políticas públicas regulatórias é observar a transparência e a participação da sociedade no processo decisório. Consultas públicas, audiências e a coleta de contribuições de especialistas, empresas e cidadãos são práticas essenciais para que as regulamentações sejam legitimadas e eficientes.

Outro ponto fundamental é a constante avaliação e monitoramento dos resultados das políticas implementadas. A adequação das regulamentações às mudanças no ambiente

socioeconômico é essencial para garantir que elas sejam efetivas e coerentes com as necessidades da sociedade.

Contudo, é importante ressaltar que a política pública regulatória não é uma solução única para todos os problemas, e seu sucesso depende de uma gestão competente e alinhada com os princípios democráticos e éticos. O excesso de regulação pode levar à burocratização e à inibição da inovação e do empreendedorismo, enquanto a falta de regulamentação pode gerar abusos, desigualdades e impactos negativos na sociedade.

Portanto, a formulação e implementação de políticas públicas regulatórias requerem um equilíbrio cuidadoso entre a intervenção estatal e a liberdade de mercado, bem como a busca constante pelo interesse público e pelo bem comum. Somente com uma abordagem responsável e informada é possível alcançar os objetivos almejados, garantindo uma sociedade mais justa, equilibrada e sustentável.

### 4.2 As limitações e as potencialidades da aplicabilidade da Lei Geral de Proteção de Dados Pessoais como forma de adaptação à brasileira

As limitações para a aplicação da política pública regulatória no Brasil são diversas e, frequentemente, encontram-se arraigadas em questões estruturais do país. A burocracia e a ineficiência estatal são obstáculos significativos que dificultam a formulação e implementação de regulamentações adequadas. A morosidade dos processos pode impedir a resposta ágil às necessidades da sociedade e do mercado.

É também comum acompanharmos o alcance das políticas públicas no âmbito jurídico, especificamente quando analisamos as decisões judiciais já que elas demonstram de modo efetivo se há de fato alguma mobilidade jurídica no atendimento aos anseios sociais mais urgentes.

Nas decisões analisadas em capítulo anterior percebemos que há uma tendência de se acionar o princípio antidiscriminatório como uma barreira para impedir a colheita genérica de dados pessoais já que no regulamento protetivo analisado é proibido inclusive o tratamento abusivo e ilícito, sinalizando assim uma tendência entre os operadores do direitos em buscar "desmistificar a figura do sujeito de direito universal em benefício de um aporte teórico-político que possibilite ao operador do direito lidar com o mundo herdado de fato, a partir da imbricação entre raça, classe, gênero, sexualidade, deficiência e colonialidade" (CORRÊA, 2021).

Contudo, este olhar direcionado à interseccionalidade ainda é escassa e uma das limitações da aplicabilidade da LGPD no Brasil se encontra na complexidade burocrática do

sistema. A adaptação das empresas e organizações às exigências da lei pode ser onerosa e demandar recursos significativos, especialmente para pequenas e médias empresas. Além disso, a conscientização sobre a importância da proteção de dados ainda é limitada entre a população, o que pode dificultar a participação ativa dos indivíduos na defesa de seus direitos.

Outro desafio reside na complexidade do sistema tributário brasileiro. A regulamentação em alguns setores pode ser dificultada por um ambiente fiscal pouco favorável, tornando as políticas mais onerosas e suscetíveis a distorções.

Desta forma, o judiciário tem sido requisitado para decidir sobre os gastos que as empresas estão tendo ao ter que se adequar a LGPD, como vemos por exemplo na decisão do TRF da 2ª Região, especificamente na apelação dos autos nº 5112573-86.2021.4.02.5101, na qual foi garantido o direito a crédito devido à adoção de medidas protetivas previstas na LGPD por uma empresa de serviços de pagamentos digitais, já que estariam diretamente relacionadas à atividade-fim da empresa.

> Tributário. Apelação. Mandado de segurança. PIS e COFINS. Regime da não-cumulatividade. Tema 779 do e. STJ. Despesas com implementação de normas previstas na Lei Geral de Proteção de Dados (LGPD). Lei nº 13.709/18. Creditamento. Possibilidade. Provimento.
> Por se tratar de investimento obrigatório, imprescindível ao alcance dos objetivos sociais da impetrante, e medida de segurança necessária à proteção dos dados dos seus clientes e de terceiros, inclusive passível de sanção pelo descumprimento da normatividade imposta, as despesas com as adequações previstas na LGPD merecem ser reconhecidas como insumos para fins de aproveitamento no sistema da não-cumulatividade de PIS e COFINS (RIBEIRO, 2023).

Em sentido contrário, o TRF da 3ª Região no processo nº 5003440-04.2021.4.03.6000 entendeu que tais gastos não seriam passíveis de creditamento, pois não estariam diretamente ligados ao exercício da atividade-fim da empresa, como consignado pelo relator:

> Não devem, no entanto, ser consideradas insumos as despesas com as quais a empresa precisa arcar para o exercício das suas atividades que não estejam intrinsecamente relacionadas ao exercício de sua atividade-fim e que seriam mero custo operacional. Isso porque há bens e serviços que possuem papel importante para as atividades da empresa, inclusive para obtenção de vantagem concorrencial, mas cujo nexo de causalidade não está atrelado à sua atividade precípua, ou seja, ao processo produtivo relacionado ao produto ou serviço.

Outro entrave para a aplicabilidade da LGPD se encontra na dificuldade de fiscalização efetiva de seu cumprimento, pois a capacidade da ANPD de monitorar todas as atividades de

tratamento de dados é limitada, pois somente em julho de 2023 que foi aplicada a primeira multa por descumprimento à LGPD.

> A Coordenação-Geral de Fiscalização da ANPD (CGF/ANPD) publicou no Diário Oficial da União de ontem (06/07) sanção decorrente da conclusão de processo administrativo sancionador contra a empresa Telekall Infoservice (acesse aqui a publicação no DOU).
> A CGF/ANPD concluiu que a empresa infringiu os arts. 7º e o 41 da LGPD, além do art. 5º do Regulamento de Fiscalização da ANPD.
> Para a infração ao art. 7º da LGPD e ao art. 5º do Regulamento de Fiscalização foram aplicadas sanções de multa simples. O descumprimento ao art. 41 da Lei resultou em sanção de advertência.
> Por se tratar de uma microempresa, o valor para cada infração ficou limitado a 2% do seu faturamento bruto, conforme art. 52, II, da LGPD, totalizando uma multa de R$14.400,00.[18]

Ao estabelecer regras claras e princípios fundamentais, a LGPD busca proteger o interesse público e garantir que os direitos fundamentais, como a privacidade e a autodeterminação informativa, sejam respeitados. Afinal, o tratamento adequado dos dados se tornou crucial para evitar abusos e riscos à segurança e à intimidade dos indivíduos em um mundo cada vez mais conectado.

Assim como outras políticas públicas regulatórias, a elaboração da LGPD contou com a participação da sociedade por meio de consultas públicas e debates. Esse processo inclusivo assegurou que a legislação refletisse as necessidades e anseios dos cidadãos, tornando-se uma conquista democrática. Além disso, a transparência na comunicação com os titulares dos dados é um princípio central da LGPD. A clareza nas informações sobre o tratamento de dados permite que os indivíduos tenham conhecimento sobre como suas informações são utilizadas, os empoderando a tomar decisões informadas sobre sua privacidade.

Com relação a regulamentação do Setor Privado, ela estabelece obrigações e responsabilidades claras para as empresas e organizações que tratam dados pessoais, independentemente de seu porte ou natureza. Isso cria um arcabouço legal que incentiva a adoção de boas práticas de proteção de dados e a cultura de responsabilidade no ambiente digital. A obtenção de consentimento explícito dos titulares, a segurança das informações e a garantia do direito de acesso e exclusão dos dados são alguns dos elementos-chave que as empresas devem observar. Essa regulamentação tem como objetivo equilibrar os interesses dos

[18] ANPD aplica a primeira multa por descumprimento à LGPD. Site: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd . Acesso em 15 de julho de 2023.

negócios com a proteção dos direitos individuais, promovendo a confiança dos consumidores e estimulando a inovação responsável.

E como consequência para o seu não cumprimento, a LGPD possui uma característica importante que é a previsão de sanções administrativas e civis para o não cumprimento de suas disposições.

Entretanto, é necessário que tenhamos em vista que a tutela de direitos não se dá apenas quando uma lesão se concretiza, de forma a reprimi-la ou ainda indenizá-la, mas que a tutela pode e deve tomar forma preventiva, inibitória ou ainda positiva para viabilizar a sua máxima realização (SCHREIBER, 2015 como citado em NEGRI & KORKMAZ, 2019).

Sendo assim, a LGPD é um marco importante para o Brasil, representando uma resposta responsável e atualizada aos desafios do século XXI, protegendo os cidadãos e promovendo a proteção de dados como um valor essencial para a sociedade contemporânea.

## CONCLUSÃO

No presente estudo, foi possível observar que a matéria de proteção de dados pessoais, em sua missão de proteção do livre desenvolvimento da personalidade, dos direitos humanos e da dignidade da pessoa humana, buscou abarcar a tutela da isonomia por meio de alguns dispositivos antidiscriminatórios no texto da LGPD, que entre eles especificamente tratamos do princípio da não discriminação abusiva e ilícita.

Leis que começaram a vigorar antes de 2018 trataram de dados pessoais de forma esparsa e limitada a alguns setores, no entanto esta pesquisa teve como base a observação da tutela antidiscriminatória amparada somente na LGPD devido ao seu alcance genérico, a sua atualidade e importância que este regulamento legislativo representa para a proteção de dados.

Com a apresentação de conceitos, contextualização de leis – onde se observou a conciliação entre práticas culturais e o alcance da tutela antidiscriminatória - e de situações que contribuíram para a inserção do princípio analisado neste ordenamento regulatório protetivo, foram apresentadas decisões judiciais que utilizaram como fundamento, entre outros, o artigo 6º, IX da LGPD a fim de garantir o enfrentamento à ilegalidade e abusividade discriminatória.

Observamos que o poder fiscalizatório da Autoridade Nacional de Proteção de Dados é um pilar fundamental para a efetividade da Lei Geral de Proteção de Dados Pessoais no Brasil, uma vez que ela desempenha papel essencial na proteção da privacidade dos cidadãos, garantindo que as empresas e organizações tratem os dados pessoais de forma adequada e em

conformidade com a legislação. Sua atuação é essencial para promover a cultura de respeito à privacidade e para assegurar que os direitos fundamentais dos indivíduos sejam preservados. A ANPD representa, assim, um importante instrumento de defesa dos cidadãos brasileiros em meio aos desafios da era digital.

Contudo, e com a iniciativa de organizações sociais e de instituições que possuem como tutela a proteção de direitos coletivos que se utilizam de ações judiciais para buscar o atendimento pleno de direitos garantidos em políticas públicas regulatórias, é no judiciário que vemos que está sendo desempenhado um papel vital na garantia do atendimento ao princípio da não discriminação, uma vez que a ANPD, responsável por orientar, fiscalizar e promover a adequada aplicação da legislação, encontra-se em estágios iniciais de operação.

O judiciário, por sua natureza independente e imparcial, pode prover uma abordagem mais dinâmica e adaptável na análise de casos que envolvem a discriminação no tratamento de dados. Além disso, as decisões judiciais podem estabelecer precedentes que orientam o comportamento de organizações e indivíduos no tratamento de dados pessoais, contribuindo para a construção de uma cultura antidiscriminatória.

Entretanto, a atuação do judiciário não deve ser encarada como uma substituição definitiva à atuação da ANPD. O desenvolvimento e fortalecimento da autoridade reguladora são essenciais para fornecer diretrizes claras e consistentes sobre como evitar a discriminação no tratamento de dados. A harmonia entre a atuação do judiciário e da ANPD é fundamental para a construção de um ecossistema jurídico que efetivamente proteja os direitos individuais e coletivos.

Sendo assim, o judiciário desempenha um papel crucial na garantia do atendimento ao princípio da não discriminação, especialmente quando a atuação da ANPD ainda é incipiente. As cortes judiciais possuem a capacidade de estabelecer diretrizes, esclarecer conceitos e prover justiça em casos que envolvem a proteção de dados pessoais e a não discriminação. No entanto, é imperativo que haja um esforço conjunto para fortalecer tanto a autoridade reguladora quanto a estrutura judiciária, visando a plena realização dos objetivos traçados pela LGPD em prol de uma sociedade mais justa e equitativa.

A aplicabilidade da Lei Geral de Proteção de Dados Pessoais no Brasil apresenta tanto desafios quanto oportunidades. Superar a burocracia, estimular a conscientização, aprimorar a fiscalização e promover uma cultura de respeito à privacidade são passos fundamentais para maximizar as potencialidades da LGPD. Ao fazer isso, o Brasil pode se posicionar como um

protagonista na defesa dos direitos individuais em um mundo cada vez mais conectado, garantindo a privacidade e a autodeterminação informativa dos cidadãos.

## REFERÊNCIAS BIBLIOGRÁFICA E ELETRÔNICAS

- ALMEIDA, Silvio. Racismo estrutural, São Paulo:Pólen, 2017.
- ANPD torna-se autarquia de natureza especial. Site: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial . Acesso em 24 de outubro de 2022.
- ARISTÓTELES. Ética a Nicômaco. Trad. Pietro Nassetti. 5ª Edição. São Paul : Martin Claret, 2001.
- BARROSO, Luiz Roberto. Razoabilidade e isonomia no direito brasileiro. In: Viana, Márcio Túlio; Renault, Luiz Otávio Linhares (Org.). Discriminação. São Paulo: LTr, 2000.
-_____. Interpretação e aplicação da Constituição: fundamentos de uma dogmática constitucional transformadora. São Paulo, Saraiva, 1999.
- BAUMAN, Zygmunt. Modernidade Líquida. 1ª Edição. Rio de Janeiro, Zahar, 2021.
- BIONI, Bruno. Proteção de Dados: Contexto, Narrativas e Elementos Fundantes. São Paulo: B.R. Bioni Sociedade Individual de Advocacia, 2021.
-BIONI, Bruno; MONAGREDA, Johanna K.; MESQUITA, Hana; ZANATTA, Rafael. Construindo caminhos para a justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais. São Paulo: Editora Data Privacy Brasil, 2022.
- BLUM, Renato Opice; MALDONADO, Viviane Nóbrega. Lei Geral de Proteção de Dados Comentada. São Paulo: Revista dos Tribunais, 2019.
-_____. Comentários ao GDPR. Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Revista dos Tribunais.
- BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF. Senado Federal: Centro Gráfico,1988.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF. Publicação em 24 abr, 2014.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Diário Oficial da União, Brasília, DF. Publicação em 15 ago, 2018.

- CARDOSO, Letícia. Uso de algoritmos em processo seletivo de emprego pode prejudicar candidatos. https://www.geledes.org.br/uso-de-algoritmos-em-processo-seletivo-de-emprego-pode-prejudicar-candidatos/ Acesso em 11 de jul, 2023.

- CAVALCANTE, Isabella; FERREIRA, Pedro. SP: Câmera de identificação facial é vetada por risco de prática racista. https://noticias.uol.com.br/politica/ultimas-noticias/2023/05/18/tribunal-suspense-cameras-reconhecimento-facial-sp.htm?cmpid=copiaecola . Acesso em 10 de jun, 2023.

- CORRÊA, Bianca Kremer Nogueira. Direito e tecnologia em pespectiva amefricana: Autonomia, algoritmos e vieses raciais. Tese (doutorado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Direito, pg. 20, Rio de Janeiro: 2021.

- COSTA, Leonardo Portugal da. A construção da Lei Geral de Proteção de Dados e seus efeitos para o Pequeno Empresário e para o Cidadão. Disponível em: https://app.uff.br/riuff/bitstream/1/13068/1/Leonardo%20Portugal.pdf Acesso em: 20 nov, 2020.

- DINIZ, Maria Helena – Compêndio de Introdução à Ciência do Direito – 6ª ed. Atual – São Paulo: Saraiva, 1994.

- DONEDA, Danilo; LEMOS, Carolina Carvalho. Decisões automatizadas nos sistemas de pontuação de crédito e o direito à explicação algorítmica do titular de dados pessoais. 2020. 193 f. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2021.

- FRANCE PRESS. (2019). San Francisco proíbe a polícia de usar reconhecimento facial Oito dos nove conselheiros municipais são contrários à tecnologia. G1,16/05/2019, online. Disponível em: https://g1.globo.com/poparte/noticia/2019/05/16/san-francisco-proibe-a-policia-de-usar-reconhecimentofacial.ghtml. Acesso em: 05 dez, 2020.

- FOUCAULT, M. Microfísica do poder. Tradução de Roberto Machado. 6. ed. Rio de Janeiro: Paz e Terra, 2017.

- FREY, K. (2000). Políticas Públicas: um debate conceitual e reflexões referentes à prática da análise de políticas públicas no Brasil, n° 21. Acesso em 01 de 08 de 2023, disponível em: http://www.ipea.gov.br/ppp/index.php/PPP/article/viewFile/89/158 .

- GUARESCHI, N. (2004). Problematizando as práticas psicológicas no modo de entender a violência. In: STREY, Marlene (Org.). Violência, gênero e políticas públicas. Porto Alegre: EDIPUCRS.

- GIL, A. C. Métodos e Técnicas de Pesquisa Social. São Paulo: Atlas, 2008.

- JUNQUEIRA, Thiago. Tratamento de Dados Pessoais e Discriminação Algorítmica nos Seguros. São Paulo: Revista dos Tribunais, 2020.
- LARENZ, Karl. Metodologia da ciência do direito. 3. Ed. Tradução de José Lamego. Lisboa: Fundação Calouste Gulbenkian, 1997.
- LATOUR, Bruno. Reassembling the Social: An Introduction to Actor-Network-Theory. New York: Oxford University Press, 2005.
- LIMA, Cíntia Rosa Pereira de. A imprescindibilidade de um órgão independente para a efetiva proteção dos dados pessoais no cenário futuro do Brasil. Tese de Livre Docência. Ribeirão Preto: FRDP/USP, 2015. 487 páginas.
- LOPES, B e AMARAL, J. N. (2008). Políticas Públicas: conceitos e práticas. Belo Horizonte: Sebrae/MG.
- LUCCA, Newton de; SIMÃO Filho, Adalberto; (coords.). Direito & Internet: Marco Civil da Internet, Lei n. 12.965/2014. 2 volumes. São Paulo: Quartier Latin, 2015.
- MAGNO, M. E. da S. P.; BEZERRA, J. S. Vigilância negra: O dispositivo de reconhecimento facial e a disciplinaridade dos corpos. Novos Olhares, São Paulo, v. 9, n. 2, p. 45-52, 2020. ISSN: 2238-7714. DOI: https://doi.org/10.11606/issn.2238-7714.no.2020.165698. Disponível em: https://www.revistas.usp.br/novosolhares/article/view/165698. Acesso em: 05 maio 2023.
-MALDONADO, Viviane Nóbrega. Lei Geral de Proteção de Dados: manual de implementação. São Paulo: Revista dos Tribunais, 2019.
- MCCANN, Michael W. Poder Judiciário e Mobilização do Direito: Uma perspectiva dos "Usuários". Revista da EMARF, Cadernos Temáticos, Rio de Janeiro, p. 1, dez. 2010.
- MELLO, Celso Antônio Bandeira de. Conteúdo jurídico do princípio da igualdade. 3. ed. São Paulo: Malheiros, 2002.
- _____. Curso de Direito Administrativo. 12ª ed. – São Paulo: Malheiros, 2000.
- MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). Revista de Direitos e Garantias Fundamentais. Vitória, v. 19, n. 3, p.164-165, set/dez. 2018.
- MUZZI, D. Tipologia de Políticas Públicas: Uma proposta de extensão do modelo de Lowi. Dissertação ISC - Escola de Gestão, 2014.
- NEGRI, S. M. C. de Á., & KORKMAZ, M. R. D. C. R. (2019). A normatividade dos dados sensíveis da lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias,* Goiânia, 5(1), 63-85. Acesso

em 29 de junho de 2021, disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479

- NUNES, Pablo. O Algoritmo e Racismo nosso de cada dia - Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/ Acesso em: 18 nov, 2020.

- _____. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. In: CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA; REDE DE OBSERVATÓRIO DA SEGURANÇA. Relatos da violência: cinco meses de monitoramento, análises e descobertas. São Paulo: Universidade Candido Mendes, 2019. Disponível em: https://bit.ly/3r6IsE3 . Acesso em: 8 maio, 2023.

- OLIVEIRA, Samuel. Sorria, você está sendo filmado!: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

- O'NEIL, Cathy. Assim os algoritmos perpetuam a desigualdade social. Portal El País– 17 abr. 2018. Entrevista concedida da Patrícia Peiró. Disponível em: https://brasil.elpais.com/brasil/2018/04/12/tecnologia/1523546166_758362.html . Acesso em: 04 set. 2021.

- O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. Nova York: Broadway Books, 2016.

- Painel LGPD nos Tribunais: Jurisprudência do 2º ano de vigência a Lei Geral de Proteção de Dados. A continuação de um propósito: panorama do uso da Lei Geral de Proteção de Dados em seu segundo ano de vigência no Brasil. Site: https://painel.jusbrasil.com.br/ , acesso em 10 de maio de 2023.

- PASCUAL, Manuel G. Quem vigia os algoritmos para que não sejam racistas ou sexistas? Disponível em https://brasil.elpais.com/brasil/2019/03/18/tecnologia/1552863873_720561.html Acesso em: 18 dez, 2020.

- PESTANA, Márcio. Direito Administrativo Brasileiro, São Paulo : Ed. Atlas, 4ª ed., 2014).

- PIRES, Luis Manuel Fonseca, juiz de direito da 3ª vara de Fazenda Pública, do Tribunal de Justiça de São Paulo. Decisão proferida no processo nº 1027876-45.2023.8.26.0053, em 18 de maio de 2023.

- REBELLO, Aiuri. https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milhoes-em-reconhecimento-facial-para-cidades-que-sequer-tem-saneamento-em-goias/. Acesso em 09 de maio de 2023.
- REALE, Miguel. Filosofia do Direito. 11. ed. São Paulo: Saraiva, 1986.
- RIBEIRO, Diego Diniz. Créditos de PIS e COFINS e gastos com LGPD: o que esperar do Carf? Site: https://www.conjur.com.br/2023-ago-09/direto-carf-creditos-piscofins-gastos-lgpd-esperar-carf . Acesso em 10 de agosto de 2023.
- ROUSSEAU, Jean-Jacques. Discurso sobre a origem e os fundamentos das desigualdades entre os homens. Trad. de Maria Ermantina Galvão. São Paulo: Martins Fontes, 1993.
- SANTOS, Raquel Gitirana Torquato dos. A Lei Geral de Proteção de Dados Brasileira: Uma política pública regulatória. In: Coletânea de Pós-Gradução, pg. 9, v.5, n.1, Políticas Públicas do Tribunal de Contas da União. Agosto, 2020.
- SARAIVA, Raquel. "Discriminação de gênero embutida em algoritmos". 2019. Disponível em: https://ip.rec.br/2019/03/08/discriminacao-de-genero-embutida-em-algoritmos/ Acesso em: 21 dez, 2020.
- SEAVER, N. Knowing Algorithms. In: VERTESI, J.; RIBES, D. (orgs.) digitalSTS: A Field Guide for Science & Technology Studies. Princeton Univrsity Press, 2019. pp.412-422.
- SCHMIDT, J. P.. Para Estudar Política Pública: aspectos conceituais, metodológicos e abordagens teóricas. Revista do Direito. V.3 n° 56, 2018, pp. 119-149.
- SCHREIBER, Anderson; SIQUEIRA, Andressa de Bittencourt; KLEE, Antonia Espíndola Longoni. Direitos Fundamentais e Sociedade Tecnológica. Indaiatuba, São Paulo: Foco, 2022
- SILVA, Mariah Rafaela; VARON, Joana. Reconhecimento facial no setor público e identidades trans: tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território. Rio de Janeiro: Coding Rights, 2021.
- SILVA, Tarcizio Roberto da; SILVEIRA, Sergio Amadeu da. Controvérsias sobre Danos Algorítmicos: discursos corporativos sobre discriminação codificada. In: Revista Observatório e-ISSN nº 2447-4266, Vol.6, n.4, Julho – Setembro, 2020.
- SILVEIRA, S. A. Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas. São Paulo: Edições SESC-SP, 2019.
- Smart Sampa: Juiz suspende compra de câmeras com reconhecimento facial em SP. Em: https://www.migalhas.com.br/quentes/386804/juiz-suspende-compra-de-cameras-com-reconhecimento-facial-em-sp. Redação migalhas. Acesso em 10 de jun, 2023.

- SOUTO MAIOR, Jorge Luiz. O direito do trabalho e as diversas formas de discriminação. Revista do Tribunal Superior do Trabalho, Brasília, v. 68, n. 2, 2002.
- SUBIRATS, J. et al. (2008). Análisis y gestión de políticas públicas. Barcelona: Ariel S. A.
- TAKAHASHI, T. (org.). Sociedade da informação no Brasil: Livro Verde. Brasília: MCT, 2000.
- TAYLOR, Linnet. O que é justiça de dados? Conectando direitos digitais e liberdades globalmente. In: Construindo caminhos para a justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais. São Paulo: Editora Data Privacy Brasil, 2022.
- VÉLIZ, Carissa. Privacidade é poder. Por que e como você deveria retomar o controle de seus dados. São Paulo: Contracorrente, 2021.
- VIDOR, Daniel Martins. LGPD e Big Data: discriminação e invasões de privacidade – parte 1. Disponível em: https://www.plugar.com.br/lgpd-e-big-data-discriminacao-e-invasoes-de-privacidade-parte-1/ Acesso em: 01 nov, 2020.
- ZUBOFF, S. (2021). A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder. (Schlesinger, G., Trad). Rio de Janeiro: Intrínseca.

## ANEXOS

### 1 - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, "Lei Geral de Proteção de Dados Pessoais (LGPD)".

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019).

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
IX - agentes de tratamento: o controlador e o operador;
X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às

liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019) Vigência
XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;  (Redação dada pela Lei nº 13.853, de 2019) Vigência
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob

amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
I - finalidade específica do tratamento;
II - forma e duração do tratamento, observados os segredos comercial e industrial;
III - identificação do controlador;
IV - informações de contato do controlador;
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI - responsabilidades dos agentes que realizarão o tratamento; e
VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019)

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III
Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV
Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento;
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
I - em formato simplificado, imediatamente; ou
II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:
I - por meio eletrônico, seguro e idôneo para esse fim; ou
II - sob forma impressa.
§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019
§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.
§ 3º (VETADO).

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV

DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei. Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
II - (VETADO);
III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)
V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)
VI - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 28. (VETADO).

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II

Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
II - a natureza dos dados;
III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
IV - a adoção de medidas de segurança previstas em regulamento;
V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.
§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.
§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.
§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.
§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Seção III
Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
I - o modo pelo qual é realizado;
II - o resultado e os riscos que razoavelmente dele se esperam;
III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

## CAPÍTULO VII
## DA SEGURANÇA E DAS BOAS PRÁTICAS

### Seção I
### Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
I - ampla divulgação do fato em meios de comunicação; e
II - medidas para reverter ou mitigar os efeitos do incidente.
§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II
Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. (Vigência)

## CAPÍTULO IX
## DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

### Seção I

Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (Redação dada pela Lei nº 14.460, de 2022)

Art. 55-B. VETADO

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V - (revogado); (Redação dada pela Lei nº 14.460, de 2022)

V-A - Procuradoria; e (Incluído pela Lei nº 14.460, de 2022)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea ‘f’ do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o

tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a

exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-M. Constituem o patrimônio da ANPD os bens e os direitos: (Incluído pela Lei nº 14.460, de 2022)

I - que lhe forem transferidos pelos órgãos da Presidência da República; e (Incluído pela Lei nº 14.460, de 2022)

II - que venha a adquirir ou a incorporar. (Incluído pela Lei nº 14.460, de 2022)

Art. 56. (VETADO).

Art. 57. (VETADO).

**Seção II**
**Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade**

Art. 58. (VETADO).

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)
I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)
II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)
III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)
IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)
V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)
VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)
VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)
VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)
IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)
X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)
XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)
§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)
§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)
I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)
II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)
III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)
§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)
Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)
I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)
II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)
IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)
V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) , passa a vigorar com as seguintes alterações: Vigência

"Art. 7º .....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília , 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER
*Torquato Jardim*
*Aloysio Nunes Ferreira Filho*
*Eduardo Refinetti Guardia*
*Esteves Pedro Colnago Junior*
*Gilberto Magalhães Occhi*
*Gilberto Kassab*
*Wagner de Campos Rosário*
*Gustavo do Vale Rocha*
*Ilan Goldfajn*
*Raul Jungmann*